Comments to the Ministry of Electronics and Information Technology (MEITy) on the draft Personal Data Protection Bill 2018, dated 27 July 2018, submitted by the Committee of Experts on a Data Protection Framework for India

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

In this document, we present our comments on the draft Personal Data Protection Bill 2018 (hereafter "the draft Bill") in response to the call for comments from the public by MEITy (Ministry of Electronics and Information Technology, 2018).

We are deeply concerned that the draft Bill, in its current form, fails to provide adequate user protection. Despite speaking in the language of empowerment and fiduciary responsibility, the draft Bill fails to give users a wide set of rights or incentivise effective, user-focussed grievance redress by data fiduciaries. The legal obligations on data fiduciaries' require greater detail and clarity to ensure they are meaningful and not merely broad aspirations. The emphasis on consent as a ground for processing in the new regime risks continuing the unfair burden on consumers to make decisions about their personal data when operating under information asymmetries. Without these and other concerns (set out in our response) being addressed, the draft Bill could miss the opportunity to fulfil the aspirations set out in the final report of the Committee of Experts. We welcome this attempt to erect a much-needed data protection law for India but urge further development of the draft Bill to arrive at a truly user-protecting framework.

Our comments are presented in two sections. In the first section titled "I. Overarching Comments", we raise eleven overarching concerns about the draft Bill. In the second section titled "II. Section-specific Comments", we provide section-by-section feedback and proposals on particular provisions of the draft Bill. The thinking presented here builds on our past work on the principles and design required for an effective, consumer-friendly data protection framework that takes into account the unique exigencies of the Indian context.[2]

[1] Dvara Research (formerly the IFMR Finance Foundation) has made several contributions to the Indian financial system and participated in engagements with many key regulators and the Government of India. We were the technical secretariat to the RBI's Committee on Comprehensive Financial Services for Small Businesses and Low Income Households (**CCFS**) Chaired by Dr. Nachiket Mor. We also acted as peer reviewers for the customer protection recommendations made by the Financial Sector Legislative Reforms Committee (FSLRC). Our research has been cited by the Committee of Experts on Data Protection in their White Paper (hereafter "the White Paper") of 27 November 2017 and in the Committee's final report titled 'A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians' dated 27 July 2018 (hereafter "the final report").

[2] See further, Dvara Research's response to the Committee of Experts on Data Protection (Dvara Research, 2018a) and the accompanying draft legislative document produced to support the submissions titled the Data Protection Bill, 2018 (hereafter "the Dvara Bill") (Dvara Research, 2018b). *See also* a working paper on the Effective Enforcement of a Data Protection Regime (Dvara Research, 2018c).

Table of Contents

SECTION I. OVERARCHING COMMENTS

In this section we summarise eleven significant issues of concern in the draft Bill. These are grouped into (i) foundational concerns, (ii) user protection concerns and (iii) transparency and accountability concerns. At the outset, we note that it is important to attain clarity in order for a future legal framework to be coherent and consistent.

Foundational concerns

1. **The aspiration for a "data fiduciary" paradigm falls short in application:** On the surface, a key innovation of the draft Bill is to term individuals "*data principals*" and the entities that decide to process their data as "*data fiduciaries*". The final report of the Committee explains this terminology as being driven by fairness—specifically, that people share personal data with companies based on a **fundamental expectation of trust** that their data will be used fairly in a manner that fulfils their best interest (*see* page 8 of the final report). In Indian law, the fiduciary relationship is "*a relationship in which one person is under a duty to act for the benefit of the other"* (Reserve Bank of India v. Jayantilal N Mistry, AIR 2016 SC 1). This goes beyond a mere obligation not to misuse data. It creates a distinct legal relationship whereby the fiduciary must act in utmost good faith in the best interests of the person to whom the duty is owed (Birks, 2014). Investment advisers, doctors and lawyers are among those to whom this standard applies.

   Unfortunately, despite stating this aspiration, the draft Bill does not embed comparable obligations for data fiduciaries towards their data principals. Obligations in Chapter II (*Data Protection Obligations)* and Chapter VII (*Transparency and Accountability Measures)* do not require a consideration of the interests of data principals prior to processing. The draft Bill creates high barriers to the exercise of data principal rights (detailed in our comments to Chapter VI below) and unwieldy grievance redress provisions that disempower data principals and fail to create pressure on data fiduciaries to act in data principals' interest. Although the draft Bill uses the language of fiduciary responsibility, the substantive provisions fail to articulate the higher protections and standards of conduct central to a fiduciary relationship. This misses the opportunity to realise the stated aspiration of the Committee in the final report, of creating a viable "*fourth path"* to data protection relevant to the Global South and distinct from the American, European and Chinese models. The draft Bill must clearly and unambiguously raise the performance of provider obligations to a fiduciary standard.

2. **The definition and usage of "harm" in the draft Bill limits user protections and rights**: "Harm" as currently defined sets out a wide variety of unrelated consumer injuries that may not always be a consequence of a misuse of personal data. It fails to articulate a clear conceptualisation of harms for the purposes of data protection. The current formulation is problematic for several reasons (expanded upon in our response to the section 3(2) in section II below). It casts a wide net through its list of the types of treatment that would constitute harm *without* providing a definition or formulation to explain how to interpret the list or the relationship between types of treatment on the list. The absence of a conceptual definition of harm creates many problems under the rules of statutory interpretation, including the risk that

it excludes future, unforeseen data harms that are currently not contemplated by the list. The draft Bill also defines "*significant harm*" as "*harm that has an aggravated effect"*, further exacerbating this lack of clarity.

This is a major concern because of the wide usage of harm in the draft Bill. Our analysis shows that fifteen provisions of the draft Bill, are predicated on the occurrence/likelihood of harm or significant harms (for further analysis see our response to the section 3(2) in section II below). This also means data principals have to establish an occurrence or likelihood of occurrence of harms and significant harms to exercise their rights and avail of several protections afforded to them. For instance, data principals can only raise grievances for violations that cause "harm" (section 39 of the draft Bill). Separately, data fiduciaries are obligated to notify data breaches only if they are likely to cause "harm" (section 32 of the draft Bill). Given the absence of clarity in the definition of "harm" and "significant harm", it is highly problematic to have rights and obligations predicated upon proving the existence of harm. In any event, rights or protections afforded under the data protection regime **should not be** contingent on a determination of likelihood of occurrence of harm. Substantive obligations and rights must exist irrespective of "harm" and exist to create normative protections that go beyond merely limiting harm.

Instead, we propose that (1) the draft Bill should include a broader definition of "harm" in a way that allows future jurisprudence and data practice to develop, and (2) avoid using "harm" as a threshold or trigger for any substantive obligations or entitlements under the draft Bill. Instead, a broad "right against harm" which imposes a reasonable obligation on data fiduciaries to avoid causing harm would be a good starting point to protect users and incentivise better data practice, without the confusion and potential impunity that might arise from the current formulation.

3. **The potential to create a clear, non-derogable standard for "fair and reasonable" processing needs to be fulfilled**: The draft Bill creates an obligation (in section 4) on all data fiduciaries to process personal data in a "*fair and reasonable manner*" that respects the privacy of the data principal. The inclusion of this overarching obligation is welcomed, especially as no derogations from this obligation are allowed even where data fiduciaries claim exemptions (under Chapter IX of the draft Bill). Violations of this obligation can attract penalties up to Rs. 15 crores or 4% of worldwide turnover. However, we are concerned that the absence of any clear criteria as to what constitutes "fair and reasonable" for the purposes of this draft Bill could preclude the ability of the proposed Data Protection Authority (henceforth referred to as "DPA") to effectively enforce the provision and the ability of data fiduciaries to comply with the requirement.

   We propose that this obligation should require data fiduciaries to balance their interests in processing the personal data with the impact of the processing on the interests and rights of the data principal. Support for such balancing is available in the draft Bill itself, albeit in a different context in section 17 (*Processing of data for reasonable processes*). In that provision, the DPA can take into account the interest of a data fiduciary, public interest in processing and the effect of processing activity on the rights of the data principal when deciding if certain activities count as "reasonable processing". Regulation in other jurisdictions also require assessments of fairness of processing activity by considering the impact on the rights and interests of the data principals (Information Commissioner's Office, 2018). A balancing test of

this nature would uphold the fiduciary relationship as well by ensuring data fiduciaries act in the best interests of data principals.

User protection concerns

4. **All user data should have the same standard of protection**: Reiterating our previous submission to the Committee, we do not believe that personally identifiable information should be categorised into "sensitive personal data" and "personal data" with different levels of protection for each. All personally identifiable data should be protected at the same level by the future data protection law. The value of this distinction is questionable. First, the sensitivity of personal data is heavily contextual i.e. information that is sensitive in one context and for one purpose, may not be sensitive in another. Second, modern data aggregation technologies are capable of revealing sensitive information from the processing of seemingly non-sensitive personal data. Third, newer types of data are being created through technological advances, and a list-based approach would require a future regulator to constantly update such a list. In practical terms, categorisation as "sensitive personal data" in the draft Bill merely creates limited additional obligations for data fiduciaries (requiring better forms of consent, a stricter justification for use of the data and higher punishment for misuse). Apart from creating more segmented or complex compliance obligations for entities, it is unclear whether the distinction actually results in additional protections for users.

5. **The draft Bill disincentivises and penalizes withdrawal of consent**: The draft Bill's pre-occupation with consent is of concern, especially given the Committee's recognition of the limitations of the notice-and-consent model in the White Paper. Although we welcome the attempt to conceptualise consent more clearly for the purposes of data protection, the impact of setting up two standards of "consent" (for the processing of personal data in section 12) and "explicit consent" (for processing of sensitive personal data under section 18) is unclear. In particular, we are concerned that the two standards can place increased burdens on users by relying on the degree to which granular user permissions are taken. Of more serious concern is the **inconsistency with regards to the ease in withdrawal of consent** (see further our response to section 12(2) and 12(5) in section II below). Despite an initial provision calling for withdrawal of consent to be as easy as compared to the ease with which it was given, section 12(5) states that upon the withdrawing of consent by a data principal, they would bear **all legal consequences** for the effects of such a withdrawal. This threat of legal consequences would be a significant disincentive for the data principal, and adversely affect their ability and ease of withdrawing consent to data processing. It could also put the data principal in a situation where their personal data is retained under duress, calling into question whether their consent can be considered "free" (Rao, 2003). Accordingly, we propose that withdrawal of consent should merely result in a simple termination of contract (and the related contract for service) to the relevant data principal and not potential liability for the data principal.

6. **Data principals are afforded a limited set of rights**: The draft Bill contains a very limited set of rights for data principals. A wider bouquet of rights is a pre-requisite for a truly free and fair digital economy, as aspired to in the preamble of the draft Bill. Our primary research on Indian data principals' experiences with the digital economy reveals that they have very few tools and little agency to exert their autonomy and protect themselves from harms and misuse of their personal data (CGAP, Dalberg & Dvara Research,

2017). Currently, the draft Bill sets out only four narrowly defined rights (see further our responses to Chapter VI, in section II below). These fall far short of the full range of user data rights available in most data protection regimes and recommended in our response to the White Paper.

If the draft Bill truly seeks to empower and protect users in India, it must take into account the imbalance of power between the data fiduciary and data principals when it comes to the use of personal data in the digital economy. Accordingly, the draft Bill should ensure the data principals "*two kinds of freedoms: freedom to enjoy certain conditions (i.e. empowerment) and freedom from certain conditions (i.e. protections against harms)"* (Chugh & Raghavan, 2017). We propose that the draft Bill should (1) expand the ambit of the rights currently included, and (2) formulate crucial user protection safeguards that are currently drafted as data fiduciary's obligations (e.g. *Privacy by design* in section 29, or *Security safeguards* in section 31), as universal rights of the data principals, in order to arrive at a full bouquet of rights required in a user-friendly legal paradigm. The full bundle of rights should include (i) right to clear, plain and understandable privacy notice; (ii) right to be asked for consent prior to data collection; (iii) right to adequate data security; (iv) rights to privacy by design (including privacy by default); (v) right to breach notification; (vi) rights relating to automated decision-making; (vii) right to informational privacy; (viii) right against harm (as defined in the Dvara Bill).

7. **The draft Bill creates high barriers to exercise the rights by data principals**: In order to exercise even the limited set of rights vested in data principals (other than the *right to be forgotten*, in section 27), the draft Bill requires them to (i) make written applications to the data fiduciaries, together with satisfactory identification documents and (ii) pay a fee determined by the data fiduciary. The data fiduciary can deny the request upon a unilateral assessment that doing so could cause harm to other data principals. These design choices presuppose the data principal to be a literate, educated and empowered individual who is capable of investing the time and money costs in this process to exercise their own rights. They are particularly unsuited for the Indian context.

   We call for the draft Bill to mandate that entities using personal data make themselves easily accessible to users. The objective must be to aid users' control over dissemination and quality of their personal information, rather than the reverse. Data principals should be able to approach data fiduciaries through diverse media including toll free numbers, postal mails and personal visits; fees if any should be nominal. Data fiduciaries to use the least onerous means to determine identity of data principals, and the draft Bill can specify categories of identification documents that can be provided as a minimum. The rejection of requests must be justified and referred to grievance redress mechanisms of data fiduciaries.

8. **The grievance redress framework is burdensome and limited for users**: The draft Bill requires data principals to identify a violation of the draft Bill and establish harm (or potential for harm) in order to raise a grievance. This places excessive burden on data principals to understand the statutory framework and to establish harm (which, as previously discussed, itself is a poorly defined term in the draft Bill). This precludes the ability of data principals to seek recourse where (i) a violation of the draft Bill has occurred without a manifested harm, or (ii) where the data principal may have suffered harm due to misuse of their data, despite an apparent compliance with the provisions of the Act by the data fiduciaries. In any event,

the right to privacy as a constitutional right is intrinsically valuable and data principals should have a wide entitlement to raise a grievance where they suspect their privacy rights are violated by a data fiduciary in ways not contemplated by the draft Bill, irrespective of manifested "harm". We recommend that the filing of grievances should be a simple and accessible process to encourage the data principal to engage with the system (See further our response to section 39 of the draft Bill in section II of this response).

Transparency and Accountability Concerns

9. **Data breach notifications are not mandatory but based on data fiduciaries' determination of "harm"**: Currently, section 32 of the draft Bill only requires notification to the DPA of a breach of personal data where a data fiduciary makes a subjective assessment that it is likely to cause harm. The DPA will then determine whether data principals should be notified of the breach (based on the severity of harm or if action is required on part of the data principal to mitigate such harm). This raises many concerns. First, as previously discussed the lack of clarity on the definition of "harm" makes it a poor trigger for such an obligation. In any event, there would be an incentive misalignment if companies suffering breaches were given an option to make subjective decisions on whether to report a breach. Finally, it also creates a bottleneck at the DPA where data fiduciaries need to inform data principals to take immediate action to protect themselves in the aftermath of a breach.

   Instead, we propose that the data fiduciaries should mandatorily report all data breaches to the DPA and have the freedom to reach out to data principals where direct actions are required to protect themselves. The requirement for organisations to notify their data breaches can encourage them to implement higher security standards (University of California-Berkeley School of Law, 2008). This can further encourage market competition around security practices of data fiduciaries. Notifications should be recorded in a centralised publicly available breach registry. This can enable better monitoring of the market, more research and analysis and improve supervisory capacities (see further our response to section 32 of the draft Bill in section II of this response).

10. **Accountability mechanisms of the proposed Data Protection Authority must be strengthened**: The DPA envisioned by this draft Bill is a powerful body with access to a range of enforcement tools, including the launch of investigations, levying of civil penalties and criminal punishment. However, the design of the DPA fails to incorporate many of the core accountability features required in order to ensure these powers are used appropriately. Our call for a wide set of enforcement tools was predicated on a "responsive regulation" framework (cited in the final report of the Committee) that requires a measured and transparent escalation of sanctions, from softer enforcement tools to harder actions for entities that infringe a data protection regime (Dvara Research, 2018c). Such a system must be based on clear feedback loops and criteria for exercise of supervisory judgment, and strong accountability mechanisms including clear monthly and annual reports on enforcement to a Management Board (Dvara Research, 2018c).

    We strongly recommend that the draft Bill clearly articulate a board-led governance structure for the DPA, comprising of whole time and independent members. This board-led structure will serve as an internal accountability lever for the senior leadership, therefore imparting greater legitimacy and transparency to

the decision making of the body (ITU-infoDev, 2018). The requirement to create regional and zonal bodies should be included in the law, rather than leaving it to the discretion of the DPA. The Chairperson should present annual reports on enforcement actions and monthly reports on complaints acted upon. Our comments in response to Chapter X of the draft Bill set out in detail other accountability measures that would help ensure the DPA is a more responsive body with adequate fetters on its discretion.

11. **Inconsistency in delegation of powers**: The draft Bill is an ambitious document that deals with several aspects of data protection from principles and rights, to cross-border flows and enforcement. We humbly submit that there appear to be some inconsistencies in the level of detail and delegation in the primary legislation on some of these aspects, that would benefit from further refinement. In accordance with the principles of constitutional and administrative law, the delegation of powers to bodies responsible for the implementation must be done in a definitive and consistent manner in the primary legislation (Shukla, 2003). Delegation must also not be excessive. This can be tested in a law on two grounds, "*(i) whether it delegates essential legislative functions or powers, and (ii) whether the legislature has enunciated its policy and principle for the guidance of the delegate."* (Shukla, 2003). Some provisions of the draft Bill do appear to raise concerns regarding whether they set out enough detail at the level of primary legislation (for instance, section 4 on fair and reasonable processing) or sufficient clarity and guidance policy and principle for the guidance of the delegates (for instance, section 41 on cross-border transfers). Likewise, the overlap between the DPA's and Central Government's mandate and powers in the draft Bill would benefit from clarification.

In conclusion, we note that the draft Personal Data Protection Bill 2018 is an ambitious document charting out a framework for India's future law. To ensure it fulfils its ambitions to be a "fourth way" in data protection, it however needs to address certain important concerns and inconsistencies. We submit our concerns on this version of the draft Bill, and in the subsequent section II of this document provide section-by-section comments against the corresponding section number in the draft Bill to aide in the development and evolution of the draft Bill towards a more user-protecting framework. We welcome engagement or further questions on any of these responses.

SECTION II. SECTION-SPECIFIC COMMENTS

We have listed our item-wise comments in the table below, referenced against the corresponding chapter and section of the proposed Personal Data Protection Bill.

COMMENTS:

We have listed our comments in the table below, referenced against the corresponding chapter, section number and page number of the draft Bill.

Sl. No.	Section No.	Page No.	Comment
Chapter I: Preliminary			
1.	3(3)	2	This sub-section defines anonymisation to mean an "irreversible" process by which the data principal can no longer be identified using the personal data in question. The sub-section also allows for standards of anonymisation to be specified by the DPA. It is submitted that the standard of absolute irreversibility is an unachievable standard for anonymisation. We understand that while there are various methods available to anonymise a data set, there are also many techniques available to reverse this process (Al-Azizy, Millard, Symeonidis, Keiron, & Shadbolt, 2015). There is continuous development of new techniques for re-identification or de-anonymisation as well. (Narayanan & Shmatikov, 2008) (Sébastien Gambs, 2014). With continuous development of technologies in this field the possibility of reversing the process of anonymisation cannot be removed completely. A method of anonymising data which meets the standards of anonymisation today may become vulnerable to new techniques of re-identification in the course of time. Accordingly, imposing a standard of irreversibility may not be feasible. Personal data, as per sub-section 3(29) of this draft Bill, refers to any data "*about or relating to a natural individual who is directly or indirectly identifiable"*. It is submitted that, a similar standard of 'identifiability' should be used to define the process of

Sl. No.	Section No.	Page No.	Comment
			anonymisation as well. This means that the law would require anonymisation to the level that personal data is no longer identifiable. Accordingly, any data which has undergone the process of anonymisation would fall outside the definition of personal data and thus outside the purview of this law.
2.	3(9)	2	This sub-section defines a "child" as a data principal under the age of 18. The related provisions under Chapter V (*Personal and Sensitive Personal Data of Children)* include obligations for data fiduciaries dealing with children's data (such as a requirement to obtain consent for using personal data or sensitive personal data of a child from a parent or guardian). It is submitted that the inclusion of a single, flat threshold that limits children's ability to access data-driven services without the oversight of parents or guardians could be very restrictive, given the evolving context of modern life. The threshold of 18 years of age is in itself not a consistent threshold even across Indian laws. While 18 is the recognised age of attaining majority as per Indian Majority Act 1875 and the minimum age to enter into a contract according to section 11 of Indian Contract Act 1872, there is precedence in other laws prescribing different age limits. For example, Section 89 of the Indian Penal Code considers the age of 12 to be relevant in order to obtain consent from an individual when conducting a medical examination or treatment (Mathiharan, 2014). Meanwhile, the Reserve Bank of India allows minors between the age of 10 and 18 to operate bank accounts independent of their parent or guardian (Reserve Bank of India, 2014). Outside of India, Article 8 of the European Union's General Data Protection Regulations (henceforth "EU GDPR") sets the age of lawful consent at 16, while also allowing for members states to reduce it to the age of 13 (EU Regulation 2016/679, 2016). The Australian Privacy Principles Guidelines allows an entity to presume that "*an individual aged 15 or over has the capacity to consent, unless there is something to suggest otherwise*" (Office of the Australian Information Commissioner, 2018).

Sl. No.	Section No.	Page No.	Comment
			Accordingly, we note that the age limit prescribed in this sub-section may be too high considering the fact that a large number of minors actually utilise various digital services which require the processing of their personal data. Various social media sites, like Facebook, set a minimum age of 13 for accessing their services. A survey conducted by ASSOCHAM suggested that 73% of minors in the age group of 8-13 in tier-I and tier-II cities use Facebook and other social networking sites (ASSOCHAM India, 2014). Modern digital platforms allow children to access to a wide variety of information, provide opportunities for learning, and also economic opportunities (UNICEF, 2017). Restricting access to the digital economy for all children or making it subject to the oversight of parents or guardians, may have unforeseen consequences. While digital safeguards for child protection should be encouraged, it is submitted that, especially for older children the age threshold and related obligations should be reconsidered and be more nuanced or graded.
3.	3(13)	3	This sub-section defines a data fiduciary to be an entity or individual who "*determines the purpose and means of processing of personal data"*. We propose that the definition of data fiduciary should also include any entity or individual who "*collects personal data from an individual prior to or during the performance or provision of a service or product, or when entering into a contract".* This framing is important because from the users' perspective it would be virtually impossible to ascertain the difference between a data fiduciary or a data processor in their interactions. For instance, with the continuous modularisation of services, a data fiduciary may appoint a third party to collect personal data from the data principal. Consumers may also come into contact with entities acting on behalf of the ultimate data fiduciary in the course of the delivery of a service. As per the draft Bill, such a third party would primarily be governed by the contract it has with the data fiduciary (as per Section 37 of this draft Bill). However, an entity that directly interacts with data principals is likely to have a high level of influence on the data principal and should be held to a higher standard of responsibility. Any

Sl. No.	Section No.	Page No.	Comment
			consumer-facing entity's processing will have the highest risk of infringing privacy and data protection if processes and safeguards are not in place. Accordingly, we propose that the definition of data fiduciary should be expanded to cover consumer-facing entities.
4.	3(21)	3	This sub-section defines harm by providing a list of different types of harm. This term (in combination with the term "*significant harm*") is used in seventeen other provisions of this draft Bill. This definition of harm is a matter of concern due to the following reasons. (i) The definition provided **does not link harm to the compromise of a data principal's personal data**. The harms that have been listed in this sub-section could be caused by factors unrelated to the misuse of personal data of an individual. For example, under the current definition for the term, any discriminatory treatment or loss of employment would be considered harmful. (ii) Given fast development of data processing technologies, it may be possible that newer forms of harm emerge in future which are not covered by the list provided as part of this definition. The definition does not provide any underlying principle on the basis of which newer forms of harm which may be included in this list. The list of different types of harms, provided in this sub-section, also does not conform to any particular pattern or may be considered as a class of harms. Such a pattern may be used by the future regulator or other adjudicators to interpret any new type of harm using the doctrine of *ejusdem generis.* (iii) The list-based definition of harm also includes "*any observation or surveillance that is **not reasonably expected** by the data principal."* The use of the doctrine of reasonable expectations in the context of privacy is problematic. The test of reasonable expectations is *"inherently uncertain because reasonable expectations of privacy vary across social groups, time and social culture. the boundaries of what amounts to a reasonable expectation of privacy shift over time"* (Barocas & Selbst, 2016). This uncertainty in peoples' varied reasonable expectations introduces a subjective element which could be abused in this context.

Sl. No.	Section No.	Page No.	Comment
			Apart from the above concerns with the definition of harm, the usage of harm in this draft Bill is also a major concern. (i) Sub-section 28(5) of the draft Bill allows a data fiduciary to deny the rights of a data principal provided in Chapter VI of this draft Bill if such compliance would harm other data principals. (ii) As per section 32 of this draft Bill, a data fiduciary is obligated to report a data breach to the DPA only if such breach is likely to cause harm. (iii) Similarly, as per section 39, a data principal may raise a grievance only when a violation of the provision of this draft Bill has caused or is likely to cause harm. (iv) Section 32 of the draft Bill requires a data fiduciary to undertake a Data Protection Impact Assessment (henceforth referred to as "DPIA") when there is a risk of significant harm to data principals. Such usage of the concept of harm as a condition for triggering of obligations or raising complaints is deeply problematic due to the lack of clarity of what constitutes harm in the context of the processing of personal data. There is still much debate around a comprehensive definition of harms in the context of a breach or misuse of personal data, due to various factors like the intangible nature of such harms or the fact that such harms may not immediately manifest (Solove & Citron, 2016). The use of the concept of harm brings in an element of subjective assessment to determine whether harm has occurred or is likely to occur. Based on this subjective assessment, a data fiduciary would determine whether a particular provision of the draft Bill is applicable or not. For example, a data fiduciary may reject a grievance raised by a data principal on the basis of an assessment that the data principal is not likely to suffer any harm. Accordingly, it is submitted that such usage of the concept of harm, combined with the concerns raised around the definition of harm, may result in unforeseen problems which would hamper the protection of personal data. In our response to the Committee of Experts on Data Protection (Dvara Research, 2018a) and the accompanying draft legislative document produced to support our submissions titled Data Protection Bill, 2018 (Dvara Research, 2018b), a wider definition of "harm" had been proposed, and linked to a right against harm (see section 13 of the Dvara Bill). It had been proposed that harm be defined as "*actual or potential injury or loss to an*

Sl. No.	Section No.	Page No.	Comment
			individual, whether such injury or loss is economic or non-economic, quantifiable or non-quantifiable" (see section 2(m) of the Dvara Bill). This definition drew on theory and practice around consumer harm developed by other regulators such as the US Federal Deposit Insurance Corporation (US Federal Deposit Insurance Corporation, 2017). In addition, it draws on emerging thinking on data harms being developed by jurists in the context of data regulation (Solove & Citron, 2016). Our response to the Committee of Experts had also proposed the inclusion of a right against any harm that may be caused by the processing of personal data of a data principal. In section 13 of the Dvara bill, we had proposed as part of the right against harm that "*Every entity shall make reasonable efforts to ensure that personal data is not used, disclosed or retained in ways that cause harm to individuals.*" Such a formulation obligates a data fiduciary to take reasonable steps to prevent the occurrence of any harm that may be suffered by the data principal due to the processing of personal data. Apart from this we would also like to raise a concern about sub-section 3(21)(x). In this sub-section "*any observation or surveillance that is not reasonably expected by the data principal"* is considered to be a harm. The use of the phrase 'reasonably expected' may problematically allow for an argument that any observation or surveillance that is expected by the data principal is not harmful in nature, especially because the data fiduciary could create such an expectation through its privacy notice.
5.	3(35)	5	This sub-section provides a list of the types of data that are considered as "*Sensitive Personal Data*". We reiterate our overarching submission that personal data not be categorised into "*sensitive personal*" data and "*personal data*" (as currently contemplated). This can result in each category getting different levels of protection. Sensitivity of data is heavily contextual and modern data aggregation technologies are capable of revealing sensitive information from the processing of seemingly non-sensitive personal data. Accordingly, such

Sl. No.	Section No.	Page No.	Comment
			a list-based approach to defining certain classes of data as sensitive in nature is not effective due to the following three reasons. (i) The continuous generation of newer types of data which are processed by various data fiduciaries will require the DPA to continuously keep track of new data types and determine whether such data is sensitive or not. It may not always be possible for the DPA to keep abreast of new data types and make a determination about its sensitivity. (ii) Advances in data aggregation and mining using Big Data technology often makes it possible to reveal sensitive personal data through the processing of data which has not been categorised as sensitive in nature. Such technology reduces the effectiveness of any extra protection accorded to sensitive personal data. It is possible to link information historically considered non-personally identifiable to specific individuals or devices and businesses actually have strong incentives to do so (US Federal Communications Commission, 2016). (iii) The sensitivity of data is also very contextual in nature. A variable which may not be sensitive in one context, could be highly sensitive in another. Hence, there is no objective way of determining whether a particular type of data is sensitive or not and is heavily dependent on context, as jurists like Nissenbaum have pointed out (Nissenbaum, 2004). This contextuality is also recognised in the final report of the Committee of Experts. Hence the standard of protection provided by this draft Bill should be the same for all types of personal data by which a data principal is identified or identifiable.
6.	3(37)	6	This sub-section defines a term "*significant harm*" which has been used in seven other provisions of the draft bill. It is defined as a "*harm that has an aggravated effect"*.

Sl. No.	Section No.	Page No.	Comment
			The meaning that the term "*aggravated effect*" is intended to have in this context is unclear. In the absence of clarity, a subjective judgement will be required to classify a particular harm suffered by a data principal as a significant harm. The current definition does not provide any guidance or criteria with regard to what may be considered as significant harm. Such a subjective determination may reduce the effectiveness of the protection provided to data principals by the law. As noted in our response on the definition of "*harm*" proposed in sub-section 3(21), there are a number of issues around the definition of harm. The definition of "*significant harm*" will also suffer from the same deficiencies, as currently drafted.
Chapter II: Data Protection Obligations			
7.	Chapter II		Chapter II of the draft Bill sets out obligations that data fiduciaries must adhere to. The language in the Chapter clearly reflects the binding nature of these obligations through the use of words stating that the obligations "shall" and "must" be undertaken. However, obligations for data fiduciaries are also included in several other portions of the draft Bill. Chapter VII (*Transparency and Accountability Measures*) elucidates many such obligations that must be undertaken by data fiduciaries. "*Privacy by Design*" (Section 29), places the obligation of implementing such policies and measures which ensure that processing of personal data take place in a transparent manner, and that the "*managerial, organisational, business practices and technical systems are designed in a manner to anticipate, identify and avoid harm to the data principal*". Other measures to ensure transparency and accountability include the use of methods of de-identification and encryption (sub-section 31(1)(a)), notification of data breaches to the Authority when such breach is likely to cause harm to any data principal (sub-section 32(1)), undertaking of DPIA when intending to undertake a new technology to process personal data (sub-section 33(1)) and maintain records of the processing activity (section 34). It is necessary for language to be included to clearly indicate the relationship between Chapter II and other provisions in the draft Bill that set out obligations on data fiduciaries. Particularly, there should be clarity that:

Sl. No.	Section No.	Page No.	Comment
			(i) all the obligations set out in Chapter II are binding on data fiduciaries, and apply irrespective of the grounds of processing claimed by data fiduciaries; and (ii) obtaining consent from a data principal does not relieve the data fiduciary of any of these obligations.
8.	4	6	This section sets out an obligation on all data fiduciaries to process personal data in a "*fair and reasonable manner*" that respects the privacy of the data principal. The inclusion of this overarching obligation is welcomed, especially as derogations from this obligation are not allowed even where data fiduciaries claim exemptions (under Chapter IX of the draft Bill). The violation of this obligation under the draft Bill and failure to undertake "*fair and reasonable processing*" by data fiduciaries can attract penalties up to Rs. 15 crores or 4% of their worldwide turnover. This standard could serve to protect data principals even in cases where all their other rights are vacated. However, for such a provision to have teeth, it is submitted that the draft Bill should clearly define or set out criteria for what constitutes "*fair and reasonable*" processing. The absence of any criteria or a definition introduces uncertainty regarding the permissibility of actions of data fiduciaries. Failure to include clear criteria as to what constitutes *"fair and reasonable"* for the purposes of this draft Bill could preclude the ability of the proposed DPA to effectively enforce the provision and the ability of data fiduciaries to comply with the requirement. The experience of data regulators in other jurisdictions like the EU GDPR (EU Regulation 2016/679, 2016), the guidelines issued by the UK ICO (Information Commissioner's Office, 2018), the Kenyan Data Protection Bill, 2018 (The Data Protection Bill of Kenya, 2018) and the Federal Trade Commission Act 1914 (Federal Trade Commission Act, 2010) as well as Indian jurisprudence around reasonableness and proportionality could provide useful references for articulating a criteria for "*reasonable and fair processing"*.

Sl. No.	Section No.	Page No.	Comment
9.	5(2)	6	Section 5(2) of the draft Bill deals with purpose limitation for data processing. It allows data fiduciaries to process data "*only for specified purposes* ***and for any other incidental purpose*** *that the data principal would* ***reasonably expect*** *the personal data to be used for"* (emphasis added). It is feared that this drafting could greatly expand the purposes for which the data can be processed rendering the principle of purpose limitation in the draft Bill meaningless for the following reasons. (i) The usage of the term "*incidental purposes*" could be interpreted very widely, allowing the use of personal data for purposes that are only remotely related to the original purpose. It is a generally settled proposition, under purpose limitation and use limitation principles, that personal data should be used only for the primary purpose for which they are collected, with the need to collect consent again for any secondary purposes (Group of Experts on Privacy, 2012). This kind of wide drafting goes against the basic rationale of purpose limitation. (ii) Purpose specification in section 5(2) of the draft Bill is subject to the qualification of "*reasonable expectations*" of the data principal. This introduces a subjective element that could be abused. International experience has shown that the use of the doctrine of reasonable expectations in the context of privacy is problematic. For instance, it was found to have significant limitations when used in the context of protecting the privacy of infants, children and adolescents, since they may not have well developed expectations of privacy at the time it was being intruded (Barendt, 2016). The test of reasonable expectations is *"inherently uncertain because reasonable expectations of privacy vary across social groups, time and social culture. The boundaries of what amounts to a reasonable expectation of privacy shift over time. One generation may find acceptable disclosures which earlier generations would almost certainly have found a clear infringement of privacy"* (Barocas & Selbst, 2016). This uncertainty in peoples' varied reasonable expectations could introduce uncertainty in the businesses of data fiduciaries and interfere with the data fiduciaries' ability to comply with the legislation. The use of this "reasonable person" standard in Singapore's data protection law has been critiqued for the same reasons of introducing uncertainty for all stakeholders (Chik, 2013).

Sl. No.	Section No.	Page No.	Comment
			(iii) Evidence from the studies of online consumer behaviour suggests that users often *"project their reasonable expectations on privacy notices therefore mistakenly believing that the privacy notices offer them higher protection than what they actually do"* (Martin, 2015). Such behavioural biases imply the data principals are likely to believe that the practices of the data fiduciaries correspond to "*reasonable expectations",* even when data fiduciaries are holding themselves to a lower standard. To reiterate, the general standard in data protection is to limit the processing of data only for the purposes for which personal data has been collected (Group of Experts on Privacy, 2012). This is the standard in the data protection legislation of Singapore (Chik, 2013), Malaysia (Yusoff, 2011) and the EU GDPR (EU Regulation 2016/679, 2016) to name a few jurisdictions. Accordingly, it is submitted that purpose limitation in a future Indian law must not be watered down by the use of this language. It should clearly state that personal data must only be used for specified purposes for which it is collected and not be further processed in any way incompatible with those purposes.
10.	6	7	This section sets out the principle of "*collection limitation"* that data fiduciaries are obliged to comply with. The section sets out that the "*collection of personal data shall be limited to such data that is necessary for the purposes of processing."* The draft Bill's emphasis on the collection limitation principle is much appreciated. Taken together with section 10 (*Data storage limitation*) this approach would ensure that only personal data necessary for the purposes of processing can be collected and retained by any data fiduciary. **However**, this provision could be rendered meaningless if the ***loose drafting of the purpose limitation obligation*** in section 5 of the draft Bill is retained. As described in our comment above (responding to section 5 of the draft Bill), the purpose limitation provision in this draft Bill is drafted too widely, allowing any incidental purpose reasonably expected to also count as "necessary for the purposes of processing". This means companies could

Sl. No.	Section No.	Page No.	Comment
			collect all kinds of information unrelated to the specific, explicit purpose of processing under the terms of the draft Bill. Therefore, while the collection limitation provision may seem laudable on its own, taken together with the loosely drafted purpose limitation provision (in section 5) it would have very limited effectiveness. This would further limit the effectiveness of the overall data protection regime. We reiterate that: (i) personal data should only be **collected for the specific and primary purpose** for which data fiduciaries require it; (ii) **all stages of processing** activities (contained in the definition of processing in section 3(30), such as organisation, adaptation, alteration, retrieval, combination or disclosure by transmission, dissemination) should also be subject to the condition of necessity i.e. they should only use personal data where it is necessary to fulfil the specific and primary purpose for which data fiduciaries require it.
11.	8	7	This section sets out the form of and the manner in which a privacy notice should be offered to data principals. Where personal data is not being directly collected from data principals, it requires privacy notice to be offered at or before the stage of collection or *"as soon as is reasonably practicable"*. The emphasis on providing the data principal with a detailed notice is welcome. Despite their limitations, privacy notices could still prove important for enforcing an effective data regime (Federal Trade Commission, 2012). The notice offered by a data fiduciary could be used as a tool for comparing the data fiduciaries' stated and actual data processing practices and hold them accountable for their divergence.
12.	8(1)(f)	7	Section 8(1)(f) prescribes the information that the notice should contain, where the data fiduciary has not collected the data directly from the data principal. It requires the notice to provide information on "*the source of such collection, if the personal data is not collected from the data principal."*

Sl. No.	Section No.	Page No.	Comment
			It is submitted that this section should contain greater detail about the source of the data. In its current drafting this section does not adequately equip the data principals to determine if the source of the data is credible, if the quality of personal data is disputable or if the security safeguards across the two data fiduciaries are comparable. It is therefore, submitted that when data is collected from a third party, "*the notice must also provide information regarding* *i.* *the identity and contact information for such third parties;* *ii.* *the purposes of processing that information and the legal basis for such processing;* *iii.* *the categories of data;* *iv.* *the right to access such information and dispute its accuracy;* *v.* *the nature of security measure to protect the information; and* *vi.* *how long information will be retained."* This language was previously submitted in response to public consultation on the White Paper of the Committee Experts, in section 15(k) of the Dvara Bill (Dvara Research, 2018b).
13.	8(2)	8	This section of the draft Bill mandates the provision of notice in *"a clear and concise manner that is easily comprehensible to a reasonable person and in multiple languages where necessary and practicable"*. This is appreciated and welcomed. However, this language needs to be expanded for the Indian context. (i) ***Notices should communicate to those who are not literate but whose data is being collected***: Section 8(2) relies heavily on the use of text and language to communicate the terms of processing to the data principal. This creates barriers for those who cannot read or write, which is especially worrisome in the Indian context. Statistics suggest that though 63% of India's population are literate, only 21.8% have

Sl. No.	Section No.	Page No.	Comment
			access to education beyond a matriculation/secondary level (Office of the Registrar General & Census Commissioner of India, 2015); (ii) ***Updated notices should be served if terms of use change****:* This section should include obligations for the data fiduciaries to serve updated notice to data principals whenever the terms contained in the notice are materially modified or updated. Consequently, when terms of processing are updated, it is possible for data principals to not know that the data fiduciary is processing their data in a manner different from the one they had signed up for. (iii) ***Notices should be "just-in-time" and just prior to each collection****:* Though the lead-in language to the section requires the notice to be served *"no later than at the time of collection"*, the drafting could also emphasise the need for the notice to be conspicuous and timely. These features will make it easier and more likely for the data principals to pay attention to the terms of the notice. (iv) ***Notice provision should not be subject to data fiduciaries' assessment of necessity***: The inclusion of the qualifier "*where necessary and practicable"* could allow data fiduciaries to legitimise non-service of notices in multiple languages and disincentivise them from actively improving the quality of notices. This qualification should be removed. It is submitted that the notice should be accessible to every data principal in a form that is most appropriate for their literacy levels and language preferences. Data fiduciaries should be encouraged to actively design measures that make the notice conspicuous, intelligible and relevant for the data principal. Data principal's understanding of the notice is a critical component of ensuring that the consent they provide is informed. We reiterate the language previously submitted in response to public consultation on the White Paper of the Committee Experts, to give effect to the rationale above (see section 15(1) of the Dvara Bill) (Dvara Research, 2018b) for notices:

Sl. No.	Section No.	Page No.	Comment
			"conspicuous, concise, timely, updated, transparent, intelligible and easily accessible form written in clear, plain and understandable language both in English and predominant language of the individual's geographical area and, where a significant portion of the population has limited literacy skills, in a visual and written format, in a form that can be retained and provided free of cost to the individual."
14.	9(2)(c)	8	This provision lays out obligations on data fiduciaries to maintain data quality. Sub-section 9(2) sets out the considerations that should drive data fiduciaries' efforts for maintaining data quality. One of these considerations is whether the data *"is kept in a form that distinguishes personal data based on facts from personal data based on opinions or personal assessments"*. The rationale for this provision is not clear. We seek clarification on the rationale for this distinction. Other jurisdictions do not make similar distinctions. For instance, the EU GDPR's approach is that *"any information"* in the definition of personal data should be interpreted widely to include both objective and subjective information about a person in the ambit of personal data (Article 29 Data Protection Working Party, 2007).
15.	10(1)-10(4)	8	This section sets out the obligations of data fiduciaries in relation to data storage. Section 10(1) requires the data fiduciaries to *"retain personal data only as long as may be reasonably necessary to satisfy the purpose"* (of processing). This section also obliges the data fiduciary to periodically review the necessity to retain personal data in their possession and delete the personal data in a specified manner when it is no longer necessary for their purpose, under sub-sections 3 and 4. The inclusion of these obligations for data fiduciaries is much appreciated. A periodic review and deletion of datasets will reduce the system-wide vulnerability to unauthorised accesses, de-identification and other forms of data breaches.

Sl. No.	Section No.	Page No.	Comment
Chapter III: Grounds for Processing of Personal Data			
16.	Chapter III & IV		Chapters III & IV set out the *"Grounds for processing of personal data"* and the *"Grounds for processing of sensitive personal data"* respectively. Our overarching comments discuss the diminishing usefulness of this distinction between personal and sensitive personal data. Technological advances have made it feasible to generate sensitive personal data by the recombination of personal data. By recognising these distinct categories, the draft Bill creates differential standards of protection without comparable benefits.
17.	12(2), 12(5)	9	Section 12 of the draft Bill elucidates the grounds of processing personal data on the basis of consent. Under this provision, for consent to be valid, it must be free, informed, specific, clear and capable of being withdrawn with the same ease with which it was obtained. We welcome the draft Bill's attempt to conceptualise consent. However, we flag with concern the inconsistency with regards to the ease in withdrawal of consent. This inconsistency is a grave concern as it could have the effect of creating a major barrier to withdrawal of consent by every data principal. (i) Sub-section 12(2)(e) states that an essential component of valid consent is that it must be "*capable of being withdrawn*" with the ease of withdrawal of consent being "*comparable to the ease with which consent maybe given*". (ii) However, section 12(5) states that upon the withdrawing consent by a data principal, they would bear "*all legal consequences"* for the effects of such a withdrawal. The presence of such a condition would act as a severe disincentive for a data principal if and when they wish to withdraw their consent for data processing. The threat of legal consequences of such a large magnitude, should they seek to withdraw consent, would in reality severely restrict the data principal's ability to effectuate such a withdrawal. The data principal could therefore be placed in a situation where their personal data is retained under duress, calling into question whether their consent can be considered "free" (Rao, 2003).

Sl. No.	Section No.	Page No.	Comment
			From the existing framework, we find that the manner in which consent can be withdrawn does not seem as easy as the manner in which it can be given to data fiduciaries. Accordingly, it is submitted that section 12(5) must be removed, and withdrawal of consent should merely result in a simple termination of contract (and the related contract for service) to the relevant data principal. This would also make the nature of consent freer as per section 12(2)(a). We reiterate the language previously submitted in response to public consultation on the White Paper of the Committee Experts in section 6(6) of the Dvara Bill (Dvara Research, 2018b) to clarify the position on the withdrawal of consent: *"At any time, an individual shall be entitled to revoke consent and have all personal data collected by the entity returned and deleted, except as otherwise required by law. It shall be as easy to revoke consent as it is to give it."* In addition, we note that withdrawal of consent is not provided as a right under Chapter VI (*Data Principal Rights).* However, sub-section 8(1)(d) (Notice) in Chapter II mandates data fiduciaries to provide data principals with a notice, informing them about their right to withdraw consent, and the procedure to do the same. While we welcome the provision in section 8, we recommend the inclusion of a clear right relating to consent in Chapter VI. This would clarify and reconcile any inconsistencies in the draft Bill that could create a lack of clarity during the time of implementation.
18.	13(1)	10	Section 13 of the draft Bill sets out that the Parliament and the State Legislature can process personal data without consent if required to discharge a function of the State. This provision is of concern because: (i) it is unclear why the legislatures should have a separate level of access to personal data for reasons other than those available to other State institutions under section 13(2); (ii) This sub-section is also free from the qualifiers in sub-section 13(2). Non-consensual processing by the State in accordance to sub-section 13(2) is only permitted for exercising any function of the State

Sl. No.	Section No.	Page No.	Comment
			authorised by law and for providing any service or benefit or rendering any license or permit to the data principal. It is recommended that the scope of the functions of the State should be well-defined to prevent its abuse. The language from the EU GDPR which requires a determination of whether such access is necessary and proportionate to the specific purpose can be considered: "*...the processing is based on Union or Member State law which constitutes a necessary and* ***proportionate measure in a democratic society to safeguard, in particular, important objectives of general public interest****, the controller should be allowed to further process the personal data irrespective of the compatibility of the purposes*." (EU Regulation 2016/679, 2016)
19.	16	10	This section provides an employer (as the data fiduciary) access to the personal data of an employee (data principal) for the purposes of employment without the need to take their consent. The language in section 16(2) is of grave concern as it allows for employers to process employee data without consent if the employer makes a determination that it is "*not appropriate"* or involves *"disproportionate effort"* to request consent from an employee or a potential employee. We note that this section can be problematic as it introduces a unilateral and subjective assessment for employers which could be abused and consequently place employees in vulnerable situations. Employers, as data fiduciaries are privy to the personal data of individuals at various points; some instances include individuals submitting personal information at the time of applications to jobs, documentation submitted as part of job joining formalities *et cetera* (ACAS, n.a.). We acknowledge that employers have to collect and process personal data for carrying out their functions and it may be unreasonable for an employer to obtain valid consent from such data principals each time their personal data may be used. Accordingly, it is suggested that:

Sl. No.	Section No.	Page No.	Comment
			(i) consent of employees should generally be taken before employers can access employee data; (ii) where employers cannot take consent of employees: ○ some objective criteria be included to guide and fetter the discretion of employers claiming this ground of processing, so that its abuse can be avoided, and; ○ they must justify this departure in writing, filed with their Data Protection Officer or the DPA, and (iii) obligations of Purpose Limitation (section 5), Collection Limitation (section 6), Lawful Processing (section 7) and Data Storage Limitation (section 10) be strongly held in order to protect the magnitude to which employers may have access to the personal data of their employees.
Chapter IV: Grounds for Processing of Sensitive Personal Data			
20.	18(2)	12	A higher standard has been set for the processing of sensitive personal data with regards to consent. The draft Bill calls for an explicit form of consent to be taken and sets out a higher threshold for the conceptualisation of explicit consent. There are several concerns with the current language and conceptualisation of consent in this section. (i) Sub-section 18(2)(a) states that a data principal be informed of any "*significant consequences"* that may occur as a result of such processing. We note that the term *"significant consequence"* is not well-defined and not addressed in the draft Bill. (ii) The different standards of consent set out in sections 12 and 18 only serve to confound their interpretation and application. It is unclear from the language used in section 18(2), and the unusual technique of redefining the terms *"informed", "clear"* and *"specific"* for the purposes of the "*explicit consent"* under this provision. (iii) The vague nature of the specifications of section 18(2), and the existence of consent in a supposedly milder form in section 12 could result in the misinterpretation of section 8 (*Notice*).

Sl. No.	Section No.	Page No.	Comment
			(iv) To obtain "*explicit consent*" under this provision, data fiduciaries would draw data principals' attention through privacy notices. Acceptance of such a notice by any data principal would be considered as a consenting gesture simply because the contents of the notice reveal the kind of data being collected and the processing activities that would take place. However, this may result in the notices becoming verbose and compromise their clarity (See further our response to section 8 of the draft Bill). Any consent so obtained cannot be considered *valid* (sub-section 12(2)), much less *explicit* (Grannis, 2015). The existence of such language only obfuscates the giving of consent for the data principal, while also making it harder for the data fiduciary to comply with the obligations of the draft Bill. Therefore, we flag with concern the presence of dual standards of consent and reiterate that the line between sensitive and non-sensitive personal data is a very bleak one.
21.	19	12	Section 19 addresses the processing of sensitive personal data by the State to fulfil certain functions. We note that section 19 is akin to section 13 and the only point of differentiation between the two provisions is the nature of data being processed and the degree of "*necessity"* associated with them. While provisions for processing non-sensitive personal data only require for the purpose to be *necessary*, provisions for processing sensitive personal data require the purpose to be *strictly necessary*. It is unclear how the increased degree of necessity will be interpreted in this section as against section 13.
22.	20	12	Section 20 addresses the processing of sensitive personal data in compliance with law or an order of the court of a tribunal. We note that this provision corresponds with section 14 with the distinction of the degree of necessity attached to the processing activity. It is unclear whether the use of "*strictly necessary"* will translate into implementation of the same and how the distinction of higher degree of necessity in this section will be made against that of section 14.

Sl. No.	Section No.	Page No.	Comment
23.	21	12	Section 21 addresses the processing of sensitive personal data for prompt actions (severe medical emergencies, public health threats and breakdown of public order) when "*strictly necessary"*. This section corresponds with section 15 which provides for processing of non-sensitive personal data for such prompt actions. Similar to our comments on sections 19 and 20, we flag with concern that it is unclear what the addition of the word "*strictly"* means with regards to the practice of this provision.
24.	22(1)	13	Section 22 allows for the DPA to specify further categories of data as sensitive personal data on the basis of additional grounds. In addition to further categories (which is the title of the section), section 22(1) allows the DPA to specify *"further grounds"* on which personal data can be processed. This is a very wide-reaching determination, if it is interpreted as the DPA having the power to add new grounds for non-consensual processing at a later date. We flag this provision with great concern and it is advised that this section be clarified or redrafted to prevent the creation of tension around the appropriate level of delegation to the DPA.
25.	22(2)	13	Section 22(2) sets out the criteria on the basis of which the DPA may specify further categories of data as sensitive personal data on the basis of additional grounds. (i) ***"Significant harm" as currently envisioned is an unclear and subjective criterion for the exercise of the DPA's discretion****:* We note that sub-section 22(2)(a) regards "*significant harm"* as a factor of consideration for specifying additional categories of sensitive personal data. This is problematic for several reasons. We refer you to our comments on section 3(37) with regards to "*significant harm*" pointing out the flaws in the definition of the term and advising against its use as a determinative factor in other sections of the draft Bill.

Sl. No.	Section No.	Page No.	Comment
			(ii) ***"Class of persons"***: Under sub-section 22(2)(c), the DPA can consider processing that may cause significant harm to a discernible class of data principals for the purposes of specific types of personal data as sensitive personal data. The use of this term without context and clarification could create ambiguity for all stakeholders. We note that while the objectives of the Preamble of the draft Bill seek to "*protect the autonomy of individuals in relation with their personal data"*. However, the language in sub-section 22(2)(c) is about a "*class of data principals"*. If the intention is to create a legislative basis for concepts such as class action and group privacy in Indian law, this should be clearly called out in the primary legislation together with explanations and relevant definitions rather than introduced without context. (iii) ***Big data techniques could render these classifications meaningless****:* We reiterate the stance that the evolution of technology allows for seemingly non-sensitive personal data types can be combined, analysed or reprocessed to reveal sensitive personal data about data principals (Barocas & Selbst, 2016) or a class of data principals. Consequently, almost all types of personal data could in theory be reclassified as sensitive personal data by the DPA. This demonstrates that the *ad hoc* manner of defining sensitive personal data, and the dual standards of consent for different types of data (non-sensitive and sensitive personal data) are ineffective in their desired impact and implementation; it is highly recommended that this stance of the draft Bill be revisited.
26.	22(3)	13	We welcome the provision of specification of those categories of personal data that can be collected in a repeated, continuous or systematic manner for the purposes of profiling, as sensitive personal data by the DPA. In line with the reasoning above, we reiterate that seemingly non-sensitive personal data types can be combined, analysed or reprocessed to reveal sensitive personal data about data principals (Barocas & Selbst, 2016) or a class of data principals.

Sl. No.	Section No.	Page No.	Comment
			Chapter VI: Data Principal Rights
27.	-	-	This Chapter sets out a very small bouquet of rights for data principals. Our overarching comments set out the imperatives that drive the inclusion of a wider set of rights for data principals. Including a wider bouquet of rights is a pre-requisite for a truly free and fair digital economy where data principals can transact securely and confidently. This Chapter must be expanded to include the following rights: o right to clear, plain and understandable privacy notice; o right to be asked for consent prior to data collection; o right to adequate data security; o rights to privacy by design (including privacy by default); o right to breach notification; o right relating to automated decision-making; o right to informational privacy; o right against harm. The draft Bill does not include many of these rights. Some of these rights exist as obligations on data fiduciaries in the draft Bill but these are often optional or graded obligations subject to qualifications, e.g. see section 29 (*Privacy by Design),* section 31 (*Security Safeguards*) and section 32 (*Personal Data Breach).* This results in the scales being tipped against building users' autonomy and control. We submit that an expanded set of rights must be incorporated in this draft Bill, which can be acted upon to hold data fiduciaries directly responsible to their principals, and accurately reflect the underlying logic of the principal-fiduciary agent relationship, on the basis of which the entire Personal Data Protection Bill is premised. Detailed drafting suggestions to actualise these rights are set out in an example legislative document released in the period of public consultation on the White Paper on Data Protection. (see Chapter II (*Individual Rights and Protections)* of the Dvara Bill from page 7).

Sl. No.	Section No.	Page No.	Comment
28.	24(1)	14	Section 24 of the draft Bill vests a right to confirmation and access to data principals. Under this right, data principals can seek (a) confirmation of whether their personal data has been processed (b) a brief summary of this data and (c) a brief summary of the processing activity undertaken. This is a very restrictive formulation of a data access right and is unwarranted, as it only allows data principals the right to request a "brief summary" of their own personal data being held and processed. Wide data access rights are the foundation of a good data protection law and provided in South Africa (Protection of Personal Information Act of South Africa, 2013), the European Union (EU Regulation 2016/679, 2016), Australia (Privacy Ammendment (Enhancing Privacy Protection) Act, 2012) and Brazil (Advogados, 2017). There are many important reasons why a wide data access right is necessary to meaningfully protect individuals as well as ensure that a fair market develops that does not operate under perverse incentives. Some of these reasons are set out in points (i) and (ii) below. (i) ***A limited right of access will have negative implications for exercise of all rights and for data quality****:* If data principals are not given comprehensive information about their personal data and how it is processed under this right, they will be unable to exercise any of the subsequent rights vested in this Chapter. In the absence of complete details about what is held by the data fiduciary, data principals will not be able to correctly request for their information to be corrected, ported or to restrict its continuing disclosure. In the absence of a clear and wide right to access and control our personal data, several concerns arise including individuals being unable to control future iterations of the information that makes up their digital person or identity, decisions made as a result and account for how it could be used (IEEE, 2016). For instance, barriers to access would restrict individuals' ability to correct erroneous information or provide the most relevant information regarding their lives to trusted actors (IEEE, 2016). This will have negative implications for data principals and also for data fiduciaries continuing to use their data. A right to complete access to their own data is a pre-requisite for the exercise of other user data rights and a meaningful data protection regime. (ii) ***Data fiduciaries should have an onus to present complete information through a clear user interface***: Rather than restrict users' access to their own information, data fiduciaries should be encouraged to present

Sl. No.	Section No.	Page No.	Comment
			information on users' data back to them through a clear user interface that allows users to make informed choices about how their data is used. Regulators in other jurisdictions have worked with providers to arrive at ways to show users complex information in meaningful ways. In our response in January 2018 to the White Paper, we had flagged an important parallel from the financial sector is the development of the "Schumer Box" which discloses the terms and conditions of credit card agreements to help consumers easily get a snapshot of the salient points of the agreement they are entering into (DiGangi, 2018). In a qualitative study conducted in October 2017, Indian users voiced their concerns about the opacity of their data use, which could have the effect of reducing their trust in the digital ecosystem. This is an opportunity to introduce better transparency with user-friendly design to give data principals more comfort about how their information is processed, rather than limit their visibility on these aspects (CGAP, Dalberg & Dvara Research, 2017). Accordingly, this right must be redrafted to give data principals comprehensive access to their information in an intelligible format. Given the context in India, a user who makes a request to exercise such a right is likely to have overcome several barriers to do so and should have access to complete information about their data, how it is held and processed. We reiterate that the notion of the *fiduciary* requires a higher duty to data principals, to present complex information in a way that is comprehensible to a user so that they can make informed choices, and to act in their best interests. To the contrary, the current form of this right could incentivise data fiduciaries to limit the information they provide data principals which could further reduce users' capacities to exercise any of the other rights vested under Chapter VI of the draft Bill. We recommend the following language to be included in section 24 of the draft Bill (see further section 9 of the Dvara Bill, 2018) (Dvara Research, 2018b). *"**Rights to Access and Quality of Personal Data*** *(1) Every individual shall have the right to seek access to personal data from such individual or generated by or associated with that individual's personal data, which is collected, processed, used or stored by an entity, and such access will be provided:*

Sl. No.	Section No.	Page No.	Comment
			(a) upon proper identification; *(b) within a reasonable time not to exceed ten business days;* *(c) at no charge or a nominal charge;* *(d) in a reasonable manner, and through a clear user interface that allows them to make informed choices about who sees their data, how it is used, and where and how it is stored;* *(e) where possible, through the same medium in which the information was provided; and* *(f) in a form that that can be retained and is intelligible to the individual.* *(2) When access to personal data is provided, the individual shall be informed of:* *(a) The purposes of processing the information;* *(b) the recipients of such information;* *(c) whether the individual's national identifier is provided;* *(d) the period for which such information will be retained;* *(e) the right to dispute such information and request that it be corrected or erased;* *(f) the right to lodge a complaint with the Authority;* *(g) where the information was not collected from the individual, information about the source of the information;* *(h) the existence of automated decision making and profiling."*
29.	24(2)	14	We welcome the language used in this section of the draft Bill that mandates the disclosure of information to a data principal by a data fiduciary in a manner that is clear, concise and easily comprehensible. However, the use of a "*reasonable person*" standard in this clause is not appropriate, since it opens the door for a subjective determination of data fiduciaries as to a reasonable data principal. As further described in response to section 5(2) of the draft Bill in comment 9 above, international experience has shown that the use of the doctrine of reasonable expectations in the context of privacy is problematic. The test of reasonable expectations is *"inherently uncertain because reasonable expectations of privacy vary across social groups, time and social culture. the boundaries of what amounts to a reasonable expectation of privacy shift over time. One generation*

Sl. No.	Section No.	Page No.	Comment
			may find acceptable disclosures which earlier generations would almost certainly have found a clear infringement of privacy" (Barocas & Selbst, 2016). Consequently, we recommend that the clause includes certain objective criteria that such a form of disclosure should seek to achieve. For instance the draft Bill could stipulate that "*form of the information should be in an intelligible and easily accessible form written in clear, plain and understandable language both in English and predominant language of the individual's geographical area and, where a significant portion of the population has limited literacy skills, in a visual and written format, in a form that can be retained and provided free of cost to the individual*" (See section 15 of the Dvara Bill, 2018) (Dvara Research, 2018b). This criterion could be clarified and expanded through regulatory guidance on the form of such disclosure as the market evolves.
30.	25(1)	14	Section 25 of the draft Bill vests the right to correction for data principals. This is an important right that is instrumental to maintaining data quality. It has positive effects of ensuring individuals are accurately represented by their information and entities, using information that is accurate and up to date. It is therefore in the interests of all stakeholders to ensure that this right is implemented in a manner that drives more engagement from data principals to update their records, rather than create barriers. Sub-section 25(1) makes the right to correction a conditional right, by only allowing it "*where necessary, having regard to the purpose for which personal data is being processed*". This conditionality is misplaced and should be removed for the following reasons. (i) There is no clarity as to **who** makes the determination of whether correction is necessary or not. If a right is being exercised, then the data principal has clearly acted on the basis of wanting to update information and no further determination of "necessity" should be imposed.

Sl. No.	Section No.	Page No.	Comment
			(ii) In any event, it is incorrect to impose an assessment of the purpose for which personal data is being used, before allowing the exercise of this right. Moreover, under the framework of the draft Bill, data fiduciaries should not be storing any personal data if it is unrelated to the purpose of processing (see section 10 (*Data storage limitation*) of the draft Bill). Therefore, the question of such a determination cannot arise. If any further information is being retained (in contravention of proposed section 10) then the data principal should have every right to update it irrespective of its use by the data fiduciary. The nature of data use and analytics is such that all data points about a person interact to arrive at insights when processed together, or in combination with other information (Ohm, 2010). An inaccuracy in one piece of personal information can have undetected consequences for the data subject and the data principal in numerous ways that may never be discovered. Accordingly, the language including the restriction "*where necessary, having regard to the purpose for which personal data is being processed*" in this sub-section must be removed.
31.	25 (2) and 25 (3)	15	These sub-sections set out the minimum procedural requirements to be fulfilled by a data fiduciary when dealing with a request for correction, completion of updating of personal information from a data principal. Under the current drafting the data fiduciary would be free to reject the request for correction after giving their justification in writing, following which the data principal may request the disputed nature of the data to be flagged. It is submitted that this formulation places a further burden on the data principal who has already sought to exercise their rights. Instead the section should: (i) automatically require the flagging of disputed personal data by the data fiduciary upon receipt of a request for correction; and (ii) where the request is rejected, create a direct pathway for complaints to the data fiduciary's Data Protection Officer (DPO) under the data fiduciary's grievance redressal system to reduce the further burden on the data subject (who by this stage has already overcome multiple barriers to exercise of their rights).

Sl. No.	Section No.	Page No.	Comment
			This formulation must be re-drafted to ensure a meaningful right that empowers data principals to control their information and improve data quality. In its current format it can have negative consequences for data principals and the system as a whole.
32.	25(4)	15	This provision places an obligation on data fiduciaries to notify other entities to whom it has disclosed incorrect data, following the updating or correction of such data. It should be clarified that this obligation operates **at all times**, and it should not be conditional on the assessment (as per the current drafting) of whether "*such action would have an impact on the rights and interests of the data principal or on decisions made regarding them*". As noted in comments made on section 25(1) above, an inaccuracy in one piece of personal information can have undetected consequences on all data processed in numerous ways given the manner in which large data sets are analysed using various techniques. Therefore, the notification obligation must apply in all circumstances where a data fiduciary has shared inaccurate information to any third party.
33.	26	15	We welcome the inclusion of this right to data portability in the draft Bill, and the clarity on the information to be included for porting to another service provider in the sub-clauses. However, section 26(2) creates some very problematic loopholes which could result in this right becoming meaningless. Two carve-outs or "loopholes" included in this sub-section risk rendering the right to data portability meaningless. (i) The lead-in language in this sub-section restricts data principals to claiming the right to data portability only from data fiduciaries who have used automated means to carry out processing. Automated means is defined in the draft Bill to mean "*any equipment capable of operating automatically in response to instructions given for the purpose of processing data*". The use of data in analyses conducted by human

Sl. No.	Section No.	Page No.	Comment
			analysts using programmes and statistical modelling techniques that are not automated would therefore be exempt from the requirement to port data upon request, in this framing. This creates a gap that could be exploited. The language "*shall only apply where the processing has been carried out through automated means"* should be removed from this sub-section. (ii) The sub-section 26(2)(c) introduces another major loophole whereby data portability is not required to be complied with by data fiduciaries where it reveals a trade secret or is not "*technically feasible"*. This should not be included. First, trade secret laws in any case operate alongside the data protection regime and those providers who fear their infringement are free to claim this, without the need for a specific reference in this legislation. Second, the inclusion of the language on "*technical feasibility*" is vague and imprecise. This could create incentives for data fiduciaries to set up their processing activities in divergent ways to create complexities that do not make it feasible to share data. Thus, sub-section 26(2)(c) should be removed from the draft Bill.
34.	28 (1) to 28 (5)	16	This section sets out the procedure to be fulfilled for the exercise of any of the rights in this Chapter. It creates multiple barriers to the exercise of rights which is very troubling. A future law should try to improve rather than restrict the access and use of rights it is trying to vest, if it seeks to give such rights any meaning at all. (i) ***Rights can be exercised only upon submission of a request in writing***: In order to exercise a right, a data principal is required to make a written request to a data fiduciary, together with information that satisfies the data fiduciary as to their identity. This automatically creates a very high barrier to entry in our country, where only 21.8% have access to education beyond a matriculation/secondary level (Office of the Registrar General & Census Commissioner of India, 2015).

Sl. No.	Section No.	Page No.	Comment
			We propose that this section should be amended to ensure data fiduciaries must entertain any requests to exercise rights and make many channels available through modes including online lodging, toll-free calling lines, e-mail, letter, fax or in person. (Section 23(9)(a) of the Dvara Bill) (Dvara Research, 2018b) (ii) ***Rights exercised only upon providing identity information "to satisfy the data fiduciary"****:* This drafting is problematic because it creates a unilateral power for the data fiduciary to subjectively determine whether identity information provided is satisfactory to allow the exercise of rights. We therefore propose that this section be amended to allow data fiduciaries to use the least onerous means to determine identity as they see fit, and the draft Bill can specify categories of identification documents that can be provided as a minimum. (iii) ***Fee for exercise of rights****:* Sub-section 28(2) erects another barrier for the exercise of rights by allowing for the charging of a "*reasonable fee*" to data principals seeking to exercise rights of access and correction. Given the Indian context, this is another serious barrier to exercise of rights that could dissuade even pro-active users from making requests to data fiduciaries. This is very troubling especially given that data principals exercising these rights are adding to the data quality of the entire system. We submit that this provision should be removed. **Exercise of rights should be allowed at no charge or a nominal charge** (see Section 9(1) (c) of the Dvara Bill). (iv) ***No requirement to respond to requests to exercise rights promptly***: Sub-section 28(3) creates an open-ended requirement that allows the DPA to specify a "*reasonable time period*" within which request from data principals should be complied with. Instead of this formulation a clear requirement should be stipulated within which time the data fiduciary is required to respond to requests. Meanwhile, section 108(i) of the draft Bill empowers the DPA to make rules on "*the time period **within which** a data principal may file a complaint under sub section (4) of section 28*." This results in an inequitable situation where data principals could potentially have limitation periods within which their complaints need to be filed, but data fiduciaries will have no strict requirement to respond promptly to requests to exercise rights.

Sl. No.	Section No.	Page No.	Comment
			We propose that this section should be amended to stipulate that data fiduciaries must comply with requests "within a reasonable time not to exceed ten business days". (See further section 9(1)(b) of the Dvara Bill) (Dvara Research, 2018b) (v) ***Substantial burden on data principal following rejection of rights**:* Sub-section 28(4) creates a disproportionate burden on the data principal seeking to exercise rights to once again lodge a formal complaint with the DPA upon the rejection of such a right. Instead, it is proposed that in the case where the data fiduciary rejects a data principal's request to exercise a right, there must be an automatic referral of this rejection to the internal grievance redressal procedure as envisioned in section 39(3) of the draft Bill. Where there is no satisfactory resolution within 30 days of this referral, the data principal should be provided full details of how a complaint can be made to the DPA through a variety of modes including online lodging, toll-free calling lines, e-mail, letter, fax or in person (See our further responses to section 39 of the draft Bill at comment 45). (vi) ***No obligation for data fiduciary to comply with requests if potential for harm of other data principals**:* Sub-section 28 (5) of the draft Bill enables data fiduciaries to outrightly deny the rights of one data principal where they believe such compliance could harm the rights of another data principal. Whereas there are no doubt situations where other data principals could be affected by the access, correction, or porting of their information where it is inextricably linked with others' personal information, the blunt method of summarily rejecting the rights of data principals who make valid requests is an inappropriate way to address this issue. Instead we propose that data fiduciaries should be required to: (i) undertake a balancing test (using criteria such as those set out in section 17 (1) of the draft Bill) to take into account the public interest and the effects on other data principals; and (ii) seek to give effect to the right of the requesting data principal, by masking or removing the information pertaining to others who may be impacted by this request to the best extent possible.

Sl. No.	Section No.	Page No.	Comment
			A blanket power to refuse requests to exercise rights could give data fiduciaries unilateral power to refuse inconvenient requests under the ruse that they may cause other data principals harm.
Chapter VII: Transparency and Accountability Measures			
35.	29	17	Section 29 (*Privacy by Design*) of the draft Bill outlines the broad standards which should govern Privacy by Design in India. It creates obligations for every data fiduciary to implement measures that are built to ensure the protection of a principals' privacy by design. We welcome and appreciate these provisions on Privacy by Design which has become internationally recognized best practice in data regulation. In this response we note the omission of one of the well-recognised Privacy by Design principles, namely Privacy by Default. We also note that the principles covered in section 29 are broad and overarching but not specific and actionable. It appears that they will need to be operationalized through granular provisions that can be specified through the Codes of Practice (see section 61 of the draft Bill). If so, this will involve including Privacy by Design as one of the categories listed in sub-section (6) of section 61(*Codes of Practice*) where it currently does not feature. Privacy by Design is a proactive approach to privacy protection, which actively seeks to avoid data breaches and their attendant harm. This is in contrast with more traditional approaches of providing minimum standards of compliance and offering mechanisms for redress. The concept first emerged through a joint report on PET (Privacy Enhancing Technologies) by the Information and Privacy Commissioner of Ontario (Canada), the Dutch Data Protection Authority and the Netherlands Organization for applied scientific research (Hustinx, 2010). Dr. Ann Cavoukian, The Information and Privacy Commissioner of Ontario (Canada), one of the main authors of the report crystallized seven foundational principles for implementing such a regime (Cavoukian, 2011). These Principles have since been recognized by the US FTC (Federal Trade Commission, 2012) and the EU GDPR (see Article 25 and Recital 78). They have also been adopted by the International Conference of Data Protection and Privacy Commissioners through a resolution passed in 2010 (ICDPPC, 2010). These principles are listed in items (i) to (vii) below.

Sl. No.	Section No.	Page No.	Comment
			The Privacy by Design principles recommend that setting up systems that are likely to handle personal data that should, (i) ***Be proactive not reactive and preventative not remedial****:* Data processors should strive to anticipate poor privacy design and correct negative impacts pre-emptively. (ii) ***Include privacy as the default****:* All systems handling data to protect the data principal's privacy by default, i.e. automatically and without the need for any action from the user. This idea is further informed by the default provisioning (to all data principals) of clear purpose specification for the collection of data (clear, limited and relevant to activity & circumstance), collection limitation to what is strictly necessary for specified purposes, the minimization of identifiability, observability, and linkability of personal information and the limitation of use, retention and disclosure of personal data. (iii) ***Have privacy embedded into design***: Technologies should have privacy protection embedded in the design stage and not added later externally. (iv) ***Full Functionality "Positive-Sum, not Zero-Sum"****:* This principle advocates that unnecessary trade-offs between privacy and other legitimate interests and objectives need not be made, because it is desirable and possible for the realization of both. (v) ***Lifecycle Protection****:* Data privacy should be protected throughout the entire lifecycle of the data in question. There should be no gaps in either protection or accountability. (vi) ***Visibility and Transparency****:* This principle advocates that the flow of information in a system is transparent, verified and visible. Accountability, openness and compliance are required for an effective and secure system.

Sl. No.	Section No.	Page No.	Comment
			(vii) ***Respect for User Privacy****:* Privacy by design requires architects and operators to have a human centric and human friendly approach so that data subjects are informed and empowered to understand and undertake privacy decisions. Most of the foundational principles (listed above) have been covered in section 29 of the draft Bill, with the notable exception of Privacy by Default. Privacy by Default requires that personal data is automatically protected in any given IT system or business practice and does not require any action on part of the individual (Cavoukian, 2011). This has also been accepted in the EU GDPR (Article 25, Recital 78). In the Indian context, where literacy and numeracy are still limited, it becomes particularly relevant for data fiduciaries and data processors to be subject to the standard of Privacy by Default.
36.	30(1)	17	Section 30(1) of the draft Bill specifies that in-order to maintain transparency regarding practices of data processing, the data fiduciary shall share data in an "*easily accessible form*". It is proposed that the standard set out for a notice to be delivered to the data principal in section 8(2) (*Notice*) of the draft Bill should be mirrored in this section. The language in section 8 (*Notice)* provides a more actionable legal standard of comprehensibility to a reasonable person and availability in multiple languages.
37.	31(2)	18	Sub-section 31(2) of the draft Bill requires data fiduciaries and data processors to undertake a review of their security safeguards periodically and take "*appropriate measures accordingly*". It would be helpful for the draft Bill to clearly specify certain categories of practices that every data fiduciary or data processor should put in place. This would add some degree of specificity to the minimum, audit requirements relating to security (for instance, as the draft Bill sets out in section 35 (2) (*Data audits*)). The following language is suggested for inclusion to provide such a minimum-security framework for data processors. This draws on language previously submitted in response to public consultation on the White Paper

Sl. No.	Section No.	Page No.	Comment
			and the draft legislative document produced to support our submissions (see section 18(1) of the Dvara Bill) (Dvara Research, 2018b). All data fiduciaries and "*data processors, shall take security measures necessary for safeguarding and securing the personal data in their custody with due diligence including* *a) designating one or more employees to coordinate their information security program;* *b) identifying and assessing the risks to personal data in each relevant area of operation, and evaluating the effectiveness of the current safeguards for controlling these risks;* *c) designing and implementing a safeguards program, and regularly monitoring and testing it;* *d) selecting service providers that can maintain appropriate safeguards, making sure their contract requires them to maintain safeguards, and overseeing their handling of customer information; and* *e) evaluating and adjusting the program in light of relevant circumstances, including changes in their business or operations, or the results of security testing and monitoring."*
38.	32(1)	18	Sub-section 32(1) specifies the breach notification requirements of data fiduciaries to the DPA. The draft Bill requires only breaches which are likely to cause harm to a data principal to be reported. It is recommended that **all** breaches must be reported to the DPA and uploaded to a centralised breach registry. This is very important for multiple reasons which are set out below. (i) A minor breach (which does not result in a "harm" as defined in the draft Bill) can have an underlying system-wide vulnerability which may be exploited subsequently. Sharing of breaches builds intelligence which reduces vulnerabilities and loopholes at an ecosystem level (University of California-Berkeley School of Law, 2008). RBI guidelines on Cyber Security for banks takes cognizance of this principle (Reserve Bank of India, 2016).

Sl. No.	Section No.	Page No.	Comment
			(ii) The availability of data on breaches can facilitate external academic research which, along with research and analysis by the regulator, builds regulatory capacity for supervision and improves security standards. (iii) In addition to system wide intelligence on vulnerabilities, a public breach registry creates strong incentives for adequate security standards given the reputational hazard associated with data breaches (Canadian Internet Policy and Public Interest Clinic, 2008). The information also incentivises innovation in companies providing security solutions because they can demonstrate the effectiveness of their solutions. Section 19(6) of the Dvara Bill supported our submission made in response to the White Paper provides language that could be used to call for a public registry of data breaches affecting all data processors and controllers. (Dvara Research, 2018b) *"The Authority shall establish and maintain a public registry of breach notifications received from data controllers and data processors and publish all notices received on the registry."*
39.	32(2)	19	Sub-section 32(2) describes the content of the breach notification. In addition to the existing provisions, the section should additionally include the following items as constituents of the breach notification: (i) the identity of the data fiduciary; (ii) the estimated date or range of dates of the breach; and (iii) the rights available to the individual and the contact information of the entity providing the notice.

Sl. No.	Section No.	Page No.	Comment
			We reiterate our submissions in response to public consultation on the White Paper of the Committee of Experts and section 19(3) of the Dvara Bill, the draft legislative document produced to support them (Dvara Research, 2018b). It is also noted that it is very important to ensure that breach notifications should not contain any personally identifiable information of any data principal.
40.	32(5)	19	Sub-section 32(5) states that upon notification of a breach by a data fiduciary to the DPA, the DPA will determine whether the breach should be reported to the data principal (based on the severity of harm or if action is required on part of the data principal to mitigate such harm). This creates an unnecessary bottleneck. Under this approach, the DPA with limited capacity will need to examine every breach reported to it and determine if it passes the threshold specified for informing the data principal. This can cause costly delays particularly in situations where action on part of the data principal can mitigate damage caused by the breach (for instance by changing of a password). Data fiduciaries themselves have a strong incentive to limit the damage as fast as possible since it exposes them to claims and the loss of customer faith. Accordingly, it is recommended that data fiduciaries should be allowed to directly notify breaches to data principals. The DPA should in addition be able to direct the data fiduciary to undertake a notification to the data principal after its assessment where it believes there is a case to provide such notification and the data fiduciary has not already done so.
41.	34(1)	20	Sub-section 41(1) lists the categories for which the data fiduciary is required to maintain accurate and up to date information. It is suggested that the records should additionally include a database of all grievances raised by data principals along with information on consequent action taken, the justification provided, and the time taken for the response (see section 23(9) (*Grievance Redressal*) of the Dvara Bill) (Dvara Research, 2018b).

Sl. No.	Section No.	Page No.	Comment
			This will facilitate an annual audit of the grievance redressal mechanism, the justification and reasoning for which is provided in the subsequent comment on the data audits (section 35 of this draft Bill).
42.	35	20	Sub-section 35 (2) lists the criteria upon which the data fiduciary should be subject to evaluation during a data audit. It is suggested that the draft Bill should include the grievance redressal mechanism (see Section 39) as one of the items to be annually audited by a data auditor. The grievance process needs to be **fast, transparent and easy to understand** for it to act effectively as the primary point of user redress. Since any relief provided by the DPA also usually demands an initial internal complaint, having a slow, complicated or non-responsive process can frustrate users and delay realisation of entitlements under the future law. We reiterate our submissions in response to public consultation on the White Paper and section 23(9) of the Dvara Bill, the draft legislative document produced to support them. (Dvara Research, 2018b). The annual audit can monitor the handling of grievances by the data fiduciary, thus ensuring that data fiduciaries maintain best practices and are held to account when they are not. This audit shall be facilitated by an internal record of all grievances filed as suggested in our previous comment on sub-section 34(1) of this draft Bill.
43.	36	21	Sub-section 36(3) specifies the eligibility of a data protection officer (DPO). The eligibility is specified as the qualifications required to carry out functions listed under section 36(1). We believe that in addition to this a DPO should have adequate technical expertise in the field of data collection or processing. The lack of a technical capability severely limits the DPO's ability to understand the nature of processing undertaken by the fiduciary and the steps required to alter the same in order to achieve compliance with the act. Moreover, as data risks constantly evolve, DPOs need to demonstrate awareness of changes to the threat landscape and fully comprehend how emerging technologies will alter these risks (Shaw, 2017).

Sl. No.	Section No.	Page No.	Comment
44.	38	22	Sub-section 38(3)(d) of the draft Bill requires only significant data fiduciaries (specified under section 38(1)) to have a DPO. This is problematic since there is no clarity on which entities will be considered significant data fiduciaries upon the commencement of the legislation. The criteria provided for significant data fiduciaries (see section 38(1) of the draft Bill) needs to be decided by the DPA as time progresses. The DPO operationalises this draft Bill both for a data principal (as the point of contact for raising and responding to grievances) and the data fiduciary (by providing information and advice for compliance with provisions). The internal logic of the draft Bill will not be consistent if personal data is better protected with certain entities, and more open to compromise when held with others. Rather, the default should be to require a DPO for every data fiduciary with exceptions only in certain extreme cases. We reiterate our submission made in response to the White Paper of the Committee of Experts, and section 17(1) of the Dvara Bill (Dvara Research, 2018b). *"(1) Every data controller, data processor or third party shall appoint a Data Protection Officer having adequate technical expertise in the field of data collection or processing and the ability to address any requests, clarifications or complaints made with regard to the provisions of this Act."* The DPA should be empowered to determine suitable thresholds, having regard to the cost of employing a DPO, below which data fiduciaries would be allowed to share the services of a common DPO. In addition, the DPA should be free to have a requirement of a DPO for any entity irrespective of exceptions, based on its reasoned risk-based assessment.
45.	39	23	Sub-section 39 (2) of the draft Bill deals with grievance redress. It states that a data principal can raise a grievance *"in case of a violation of any of the provisions of this Act, or rules prescribed, or regulations specified thereunder,* ***which has caused or is likely to cause harm*** *to such data principal".*

Sl. No.	Section No.	Page No.	Comment
			The effect of this provision would be to exclude the possibility for a data principal to raise a grievance where: (i) a violation of the Act has taken place without a corresponding proven harm or (ii) a harm has been a caused by the data fiduciary but there has been no violation of the Act (or the data principal is not equipped or trained to detect one). This is problematic for several reasons including those set out below. (i) ***Data principals suspecting that their privacy is infringed must have recourse to grievance redress****:* In light of the constitutional right to privacy (as described in the *Puttaswamy* judgement) individual privacy is intrinsically valuable, as a postulate of human dignity and an essential part of individual liberty (Justice K.S. Puttaswamy(Retd.) v. Union of India, 2017). This stated objective of this draft Bill is "*to protect personal data as an essential facet of informational privacy*" (as noted in the draft Bill's preambular language). Consequently, data principals should have a wide entitlement to raise a grievance where they suspect their privacy rights are constrained or they are likely to suffer harm. There should be no additional requirement to prove a violation of the statute imposed to limit the filing of a grievance. (ii) ***Violations of the statute should give data principals recourse to grievance redress****:* The statutory protections provided in the draft Bill are not merely protections against harm caused by non-compliance with obligations, but positive requirements that data fiduciaries must fulfil (irrespective of harm). Therefore, there needs to be redress even in the absence of harm. Regulators including the RBI also follow this principle with their respective complaint mechanisms. RBI's Banking Ombudsman Scheme (2006) allows a complaint about any experienced deficiency in banking services indifferent to any experienced harm (see chapter 6, rule 12 (*Grounds of Complaint*)) (Reserve Bank of India, 2006). (iii) ***Burden on consumer to be well versed with statutory provisions****:* The knowledge of a violation requires the knowledge of provisions of the Act, of rights and obligations. Limitations on literacy and extent/quality of education, may make it difficult for principals to describe their grievance as a violation

Sl. No.	Section No.	Page No.	Comment
			of a specific provision. We also refer you to our extensive comments in this submission on the definitions of "*harm*" and "*significant harm*" pointing out the flaws in the definition of the term and advising against its use as a determinative factor in other sections of the draft Bill. In summary, it is suggested that such a high burden of proof (of proving violation and harm) on a data principal should not exist. It is recommended that the filing of grievances should be as simple a process as possible and that the internal resolution of grievances should be encouraged. In addition to reducing the regulatory burden, it improves user trust and can improve (and sustain) migration to the digital medium.
Chapter VIII: Transfer of Personal Data Outside India			
46.	40	23	Section 40 of the draft Bill requires every data fiduciary to ensure the storage of at least one serving copy of personal data (to which this act applies) within India. In addition, the Central Government has the power to notify some categories of personal data as "*critical personal data*" that can only be processed in a server or data centre located in India. The Central Government also has the power to exempt some categories of personal data from having a serving copy in India under this provision. We raise the following concerns regarding this provision: (i) ***Clarity on objectives****:* We note that the drafting of this section does not suggest restrictive provisions with regards to cross border transfer of personal data, but only requires a serving copy of data to be stored within the Indian territory. The objectives of the draft Bill as set out in the Preamble include (i) protecting personal data which is an essential facet of informational privacy and (ii) the growth of the digital economy. The provision of this section does not appear to directly contribute to either stated objectives of the draft Bill. These provisions instead seem to be aimed at the objective of increasing the quality of access to evidence for future investigatory actions by the State. While this may be a valid objective in other contexts and legislation, it appears misplaced in this draft Bill.

Sl. No.	Section No.	Page No.	Comment
			(ii) ***Big data techniques could render these classifications meaningless****:* Section 40(2) deems some categories of personal data as "*critical personal data*", which are categories of personal data that shall be notified by the Central Government. In effect, "*critical personal data*" would be a subset of personal data. This sub-categorisation of personal data in to "*critical personal data*" creates yet another standard of differential protection for different types of data. To reiterate our submissions in other sections of this response, this differential standard of protection is ineffective since data points can be recombined and aggregated to reveal more-protected data types. In any event, it is recommended that "*critical personal data"* be defined under Section 3 of Chapter I (*Definitions*) to clarify its status amongst the categories of "personal data" and "sensitive personal data" of this legislation. A criterion needs to be provided in the primary legislation to indicate the nature of personal data that could be notified in order to ensure that the discretionary powers in this section are exercised appropriately. (iii) ***Future dissonance between Central Government and the DPA***: We note that it is the Central Government and not the DPA that has been given the power to notify sections of personal data as "*critical personal data*". However, the DPA has the power to classify categories of data as "*sensitive personal data"* under section 22 of the draft Bill. The link between these categorisations in unclear, raising the potential for dissonance between Central Government and the DPA. Given that the DPA will have a stronger understanding of the regulated space given its day-to-day functioning, it is recommended that this notification by the Central Government be made in consultation with the DPA. (iv) ***Certainty for stakeholders****:* Section 40(3) allows the Central Government to exempt some categories of "*critical personal data*" from having a serving copy in India based on *"necessity or strategic interests of the state"*. It would be helpful and necessary to define the scope of this provision clearly in order to have more certainty for all stakeholders in the digital economy.
47.	41	24	Section 41 of the draft Bill lays down the conditions for cross-border transfer of personal data. Personal data (other than that notified as "*critical personal data*") can be transferred outside the territory of India with the consent of the data principals under the conditions set out i.e. (i) pursuant to standard contractual clauses, (ii) the Central Government's "greenlight" to particular countries, sectors or international organisations and (iii) the DPA's approval of a particular transfer. Sub-section 41(3) provides exceptions for "critical personal data" to be

Sl. No.	Section No.	Page No.	Comment
			transferred outside Indian territory in cases of prompt action and where the Central Government is satisfied of the necessity for such a transfer. (i) ***Inconsistency in section 40(2) and sections 41(1) and (3) with regard to "critical personal data"***: While sub-section 40(2) mentions "critical personal data" as categories of **personal data** notified by the Central Government, sub-sections 41(1) and 41(3) mention "critical personal data" as categories of **sensitive personal data** notified by the Central Government. We request a clarification on the definition of "*critical personal data*", as the interpretation of provisions across this Chapter cannot be properly completed in the absence of such a clarification. (ii) ***Inconsistent delegation of powers from legislation****:* This provision of the draft Bill introduces a complex schema according to which all entities must arrange their processes in order to undertake cross-border data flows. However, there are drafting inconsistencies (see above) and inconsistencies in the delegation of discretionary powers that leave the provision open to challenge. In accordance with the principles of constitutional and administrative law, the delegation of powers to bodies responsible for the implementation must be done in a definitive and consistent manner in the primary legislation (Shukla, 2003). This delegated legislation must not be excessive, and this can be tested on two grounds, "*(i) whether it delegates essential legislative functions or powers, and (ii) whether the legislature has enunciated its policy and principle for the guidance of the delegate* (Shukla, 2003)." Section 41 appears to be plagued by both ills given that certain provisions (such as section 41(3)) do not set out enough detail on policy and principle for the guidance of the delegate, whereas certain others (such as section 41 (1)) appear to delegate powers to the Central Government on some aspects and the DPA others in a manner that seems inconsistent. It is appreciated that the draft Bill cannot possibly elucidate all the details of a complex situation to result in maximum benefit and to address all the contingencies. Accordingly, it must strike a balance of providing enough substantive policy and principle for guidance of future delegates in the primary legislation, while allowing for delegated legislation to clarify the operation of the law as specialised knowledge and expertise develops in

Sl. No.	Section No.	Page No.	Comment
			context. It is in this light that delegated legislation is provided for by the substantive legislation (Shukla, 2003). The current drafting of Chapter VIII however does not seem consistent with these fundamental principles, and it is humbly submitted that the entire schema must be revisited to ensure enough clarity in primary legislation as well as appropriate distribution of delegated powers to the DPA (which will have a stronger understanding of the regulated space given its day-to-day functioning) or Central Government taking into account their relative expertise and functioning.
Chapter IX: Exemptions			
48.	42(1)	25	Section 42 of the draft Bill provides an exemption for any processing of personal data in the interests of the "*security of the state"*. The language of this provision is framed in a limited manner, stating that no data processing can be undertaken in the interests of the "*security of the state*" unless it is in accordance with "*procedure established by law*" and is "*necessary for, and proportionate to"* to such interests being achieved. We welcome the inclusion of this limiting language requiring clear safeguards before personal data can be accessed by the State in this context. The final report submitted by the Committee of Experts (on page 122), recognised that a large share of processing of personal data for security of the State is done outside the purview of *any* law and without adequate legal and procedural safeguards to protect civil liberties (Committee of Experts on A Data Protection Framework for India, 2018). Therefore, this provision is a first step towards introducing such a restraint. However, the language in the draft Bill does not fulfil the vision of the final report of the Committee in some ways. (i) ***No provision for a judicial oversight mechanism when personal data is used for the security of the State****:* The final report of the Committee recognised (on page 128) the lack of comprehensive oversight of surveillance or monitoring of data principals. The report specifically recommended that a law governing the same should be expeditiously brought into effect. (Committee of Experts on A Data Protection Framework for India, 2018). Similar oversight mechanisms exist in other jurisdictions (such

Sl. No.	Section No.	Page No.	Comment
			as the FISA court in the United States of America or the Parliamentary Control Panel in Germany) and have been discussed in the Committee's final report. The final report acknowledges the need to establish an oversight mechanism and recommends that the government should scrutinise this issue and address it through suitable legislation. (Committee of Experts on A Data Protection Framework for India, 2018). However, the draft Bill does not make any mention of such a mechanism. This appears to be a glaring omission that must be rectified. (ii) ***All relevant procedural safeguards under the Constitution will apply***: The usage of the term *"procedure established by law"* mirroring Article 21 of the Constitution follows Indian jurisprudence that does not allow any interference with the right to life and personal liberty unless a valid law justifying such interference and the procedure laid down in the law is strictly followed (see *Maneka Gandhi v. Union of India (1978 SCR(2) 621)* establishing the relationship between Articles 14, 19 and 21 of the Constitution). We note that the judgements in *Puttaswamy v. Union of India* (Justice K.S. Puttaswamy(Retd.) v. Union of India, 2017) did foresee privacy as arising across the gamut of fundamental rights in Part III of the Constitution (not limited to Article 14, 19 and 21, for instance as indicated by the reference to Article 25 and rights to Freedom of Religion). Accordingly, it must be clarified that the exemption outlined in sub-section 42(1) would be subject to the requirement to meet all the procedural safeguards that exist in the law and the Constitution before circumscribing the relevant rights in Part III of the Constitution.
49.	43(2)	26	This section provides an exemption for any processing of personal data in the interests of prevention, detection, investigation and prosecution of any offence or any other contravention of law. For data fiduciaries claiming this exemption, sub-section 43(2) provides a wide exemption from all provisions of data protection law, except for (i) the obligation of fair and reasonable processing and (ii) the obligation to implement reasonable security safeguards. Such a vacation of all rights of a data principal where a data fiduciary claims this exemption is problematic. Such a restriction of rights is not necessary for achieving the interests referred to in sub-section 43(1). Rather, rights

Sl. No.	Section No.	Page No.	Comment
			should only be restricted upon written justification that it is necessary to achieve the purposes for which the exemption is provided. The justification should restrict rights of individuals only where failure to do so would be prejudicial to the investigation or prosecution in question. This is the approach followed in other jurisdictions with success. It allows for the objectives of law enforcement and personal data protection to both be served (rather than sacrificing one for the other). A pertinent example is in the European Union Directive 2016/680 on Protecting personal data when being used by police or criminal justice authorities (EU Directive 2016/680, 2016). This directive provides several rights to individuals like right to notice, right to access, right to rectification or erasure of personal data etc. Recital 44 of the Directive says that the right of individuals to access their data may be partially or wholly restricted only when such a measure is necessary and proportionate *"to avoid obstructing official or legal inquiries, investigations or procedures or to avoid prejudicing the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties"* (EU Directive 2016/680, 2016). The directive imposes various obligations, "*on competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security*" (EU Directive 2016/680, 2016). This includes maintaining adequate security of the personal data stored, storage limitation requirements, requirement to have data protection officers, personal data breach notification requirements etc. Exemptions from these obligations **are only allowed** when it is considered necessary and proportionate (EU Directive 2016/680, 2016).
50.	43(3)	26	As mentioned above, section 43 of the draft Bill exempts the processing of personal data in the interests of prevention, detection, investigation and prosecution of contravention of the law. Sub-section 43(3) limits the use of the exemption when processing personal data of a victim, witness or any other person with information about relevant offence or contravention. When processing data of such data principals, the exemption may only be used only if processing in compliance with the law shall be prejudicial to the prevention, detection, investigation or prosecution of any offence or other contravention of law. Such an

Sl. No.	Section No.	Page No.	Comment
			exemption would allow for the processing of personal data of victims or witnesses of crime without their consent. The exemption would also restrict the ability of victims or witnesses of crimes to be able to confirm whether their data is being processed. This is a concern as it may involve information that the data principal may not want to reveal. For example, the very identity of an individual who has been a victim of rape or domestic violence is data which is highly sensitive and something which the victim may not want to reveal. Such a broad exemption would restrict the right to privacy of victims of crime. The United Nation Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power requires that measures are taken "*to minimize inconvenience to victims, protect their privacy, when necessary, and ensure their safety, as well as that of their families and witnesses on their behalf, from intimidation and retaliation"* (United Nations, 1985). In 2003, the Committee on Reforms of the Criminal Justice System, set up by the Ministry of Home Affairs Government of India under the leadership of Justice V.S. Malimath, also mentioned the need for maintaining privacy of victims and witnesses in the Indian criminal justice systems (Committee on Reforms of Criminal Justice System, 2003). It is submitted that the rights of victim, witness or any other person with information about relevant offence should not be restricted unless there is specific judicial oversight requiring written justification.
51.	45(1)	27	The section provides an exemption from various obligations under the draft Bill for any processing of personal data for the research, archiving and statistical purposes. Entities claiming this exemption can be exempted from any provisions of the draft Bill except for (i) the obligation of fair and reasonable processing, (ii) the obligation to implement reasonable security safeguards and (iii) requirement to undertake DPIA. The reason for such an exemption, as explained on page 137 of the final report submitted by the Committee of Experts, is the encouragement of free flow of information and ideas for the advancement of knowledge in public interest (Committee of Experts on A Data Protection Framework for India, 2018). However, it is noted that section 45 in the draft Bill does not have any reference to public interest. This is a significant oversight, for the reasons set out below.

Sl. No.	Section No.	Page No.	Comment
			The exemption for research purposes is well-recognised across data protection regulations in other countries. However, this is never a blanket exemption for any kind of research but only for research aimed at improving knowledge in the public interest (as opposed to research for purely commercial interests). For instance, South Africa's the Protection of Personal Information Act, 2013 provides an exemption in section 27 for processing of data for historical, research or statistical purposes provided it ***serves a public interest*** (Protection of Personal Information Act of South Africa, 2013). Similarly, Article 89 of the EU GDPR provides an exemption for research purposes but limits it to "*archiving purposes in public interest, scientific or historical research or statistical purposes"* (EU Regulation 2016/679, 2016). Accordingly, we submit that: (i) the exemption should only be provided for research, archiving or statistical purposes which serve the larger public interest. Any kind of non-academic research, like market research, carried out by any entity for commercial gains should not enjoy such an exemption from the data protection obligations; (ii) the obligation of notifying personal data breach, provided under section 32 of the draft Bill, should also continue to apply to data fiduciaries which enjoy an exemption under this section. The obligation of notifying any data breach is not likely to be too onerous on such data fiduciaries and also not impede the research activities being carried out by them. The breach notification would allow the future regulator to judge whether to notify the data principals whose data has been breached and steps that may be required to mitigate harm that may result from the breach.
52.	46(2)	28	Section 46 provides an exemption from the provisions of the draft Bill for any processing of personal data for purely personal and domestic purposes. Sub-section 46(2) limits this exemption to only such processing which does not involve any "*disclosure to the public*" or is undertaken for commercial or professional purposes. The use of the term "*disclosure to the public*" could be problematic if not further clarified, as it may restrict the usage of various services like social media if information posted on these services is considered public disclosure.

Sl. No.	Section No.	Page No.	Comment
			For example, the sharing of a photograph on Facebook by a data principal, which includes herself and her friends, could be considered as "*disclosure to the public*" of personal data of her friends. In such a situation, the current wording could raise the possibility that the data principal would not be able to enjoy the exemption provided under this section (and need to follow the provisions of the data protection law). Consequently, the wording of the personal use exemption must be clarified to avoid such unintended consequences. The final report submitted by the Committee of Experts has also recognised the existence of such higher publishing power that is available today (Committee of Experts on A Data Protection Framework for India, 2018). This is also recognised in the EU GDPR, where recital 18 of the Directive clarified that for the purposes of the regulations personal activity includes social networking or online activity (EU Regulation 2016/679, 2016). Accordingly, we submit that the wording in this exemption should be clarified to avoid unintended restrictions on services used by individuals for personal and domestic purposes.
53.	48(2)	28	Section 48 of the draft Bill provides an exemption for small entities meeting certain criteria that carry out only manual processing of personal data. The threshold for small entities to qualify for these exemptions are set out in sub-section 48(2), limiting the exemption to entities that (i) do not have a turnover higher than Rs. 20lakh in the preceding financial year (or such other lower amount as prescribed by Central Government), (ii) do not collect data for disclosure to other individuals or entities and (iii) have not processed data of more than one hundred individuals in any one day in the preceding year. The rationale for the inclusion of these flat thresholds to claim exemptions is unclear. Setting the threshold too low could inadvertently catch entities who may be the intended beneficiaries of this exemption. One recent example of such a flat threshold creating an undue burden on small entities arose in July 2017, when India shifted to a common Goods and Service Tax (GST) regime. Under the new GST regime, small businesses with annual turnover of over Rs. 20lakh are required to file quarterly tax returns. A number of reports have suggested that the cost of compliance of this tax regime is too high for micro enterprises (Awasthi, 2017) (Jethmalani, 2017). Compliance with GST has been associated with reduced liquidity, higher cost of borrowing as well as overall

Sl. No.	Section No.	Page No.	Comment
			declining sales volume among micro and small enterprises (Sinha, 2018). Accordingly, the criteria for small entities in sub-section 48(2) should be re-visited and better calibrated in the draft Bill.
Chapter X: Data Protection Authority of India			
54.	49(4)	29	This sub-section empowers the DPA to establish offices, in addition to the head office, "*at other places in India"*, with the prior approval of Central Government. While the DPA's ability to establish offices in other places is welcome, it is submitted that the requirement for regional and zonal offices should be mandatory in the design of the DPA and included in the primary legislation. A future nationwide regulator must contemplate a regional presence to effectively discharge its duties, given the complexity and vastness of the country. The regional offices could perform the functions of enforcement, investigation and grievance redress at the local level and report into a centralised database maintained by the DPA (Dvara Research, 2018c). This approach could potentially: (i) **Increase the effectiveness of the data protection regime by offering locally accessible points of grievance redress**: Regional offices offer a direct point of access to data principals, enabling them to register their complaints with greater ease in vernacular languages. This could significantly improve the use of the grievance redress mechanism. International best practices also suggest that local and multiple grievance uptake points are essential for an effective grievance redress mechanism (World Bank, 2016). A well-functioning grievance redress mechanism can in turn instil confidence in users and encourage them to approach the system more frequently. For instance, the UK's Financial Ombudsman Service (FOS) has seen a ten-fold increase in complaints registered over the last decade (Task Force on Financial Redress Agency, 2016). Regional offices could therefore simplify the process of grievance redress for the data principals, encourage them to engage with the system frequently and improve the effectiveness of the DPA's operations significantly. Moreover, frequent use of the grievance redress mechanism will also increase awareness about rights of data principals and incentivise data fiduciaries to comply with their obligations.

Sl. No.	Section No.	Page No.	Comment
			(ii) **Increase the efficiency in the enforcement and quasi-judicial functions of the DPA**: For the proposed DPA to be proactive and responsive, it will be required to conduct on-site supervision. Regional offices could increase the efficiency of on-site supervision and investigation (Dvara Research, 2018c), by maintaining and deploying regional teams for the purpose. Similarly, performing the quasi-judicial function at the regional level could save costs for adjudication for parties involved and enable the proposed DPA to respond to case-load. (iii) **Several existing Indian regulators also enforce their mandate through similar regional structures:** The Directorate of Enforcement, which is the specialized financial investigation agency under the Department of Revenue of the Ministry of Finance, runs regional offices with zonal and sub-zonal offices in smaller cities (Directorate of Enforcement, n.d.). Similarly, the Bombay Stock Exchange also handles grievance redress through over 20 Regional Investor Service Centres (Bombay Stock Exchange, 2018). It is therefore submitted that: (i) the legislation should empower DPA to establish zonal offices at the outset, for the reasons considered above. The DPA could also be vested with the power to expand to the regional level when the need arises. For an indicative structure please refer to our working paper titled "*Effective Enforcement of a Data Protection Law"* (Dvara Research, 2018c); and (ii) the DPA should be empowered to determine the appropriate location for its regional offices, independent of the Central Government. This will allow the DPA to remain agile and flexible when responding to the demand for its operations. Similar powers exist for the RBI under the Banking Ombudsman Scheme (Reserve Bank of India, 2006) .

Sl. No.	Section No.	Page No.	Comment
			These powers will allow the DPA to respond to the regional grievance load, expedite the process and gain consumers' confidence. Regional presence will also support the efficiency of the DPA's investigation and enforcement functions, as discussed above. For detailed discussions, please refer to our working paper titled "*Effective Enforcement of a Data Protection Law"* (Dvara Research, 2018c).
55.	50(1)	29	This section empowers the DPA to appoint a chairperson and six whole time members for carrying out the functions of the DPA. As alluded in the final report of the Committee of Experts, the fair and transparent appointment of members and the DPA's board-led governance structure are crucial to realizing the aspirations of the DPA operating as a, *"high powered, independent national body"* (Committee of Experts on A Data Protection Framework for India, 2018). A board-led structure will also help check the discretionary use of the wide enforcement powers vested in the DPA in the subsequent sections (sections 60, 62, 63, 64, 65 and 66) of this Chapter. Though the final report alludes to the merits of a board-led structure of governance of the DPA, the draft Bill does not clearly articulate that the six whole time members and the Chairperson will together constitute the Governing Board of the DPA. It is therefore submitted: (i) the draft Bill should clearly provide for the operation of the DPA as a collegial, management-board-led regulator. It should clearly articulate that the six whole time members together with the Chairperson constitute the board and the roles, responsibilities and powers of the Board and its members should also be clearly set out. A clear structure will be instrumental in ensuring that the DPA "*acts with independence, accountability and effectiveness to fulfil the objectives"* of the data protection regime (Dvara Research, 2018c); (ii) in addition to the six whole time members and the Chairperson, as set out in the Report, the Board of the DPA should also ensure representation of independent members (Dvara Research, 2018c). Independent members can be crucial for holding the DPA accountable for their performance and offer diverse

Sl. No.	Section No.	Page No.	Comment
			perspectives by accounting for the views of diverse stakeholders (HM Treasury and Cabinet Office, Government of United Kingdom, 2017); (iii) the governance structure should also fix responsibility on the Chairperson to consult with the Board on clearly identified matters, as set out in the terms of reference of the board. The Chairperson should also periodically report to the Board on the enforcement activities of the DPA. *"The Chairperson could be in-charge of the regulatory decision making, the management board should be primarily responsible for oversight, scrutiny and guidance on the operations of the regulator"* (OECD, 2013). Such collegial bodies are perceived as more independent (as it is less likely that all members would be influenced by the same actors, whether in the government or the private sector). The Board also serves as an internal accountability lever for the senior leadership, therefore imparting greater legitimacy and transparency in the decision making of the body (ITU-infoDev, 2018), and (iv) the conduct of members must be clearly set out, with well-identified *"requirements for accountability, including strict procedural requirements, reporting mechanisms, public consultation, and substantive judicial review"* (ITU-infoDev, 2018).
56.	53	31	This section sets out the powers of the Chairperson of the DPA. The Chairperson is vested with powers of "*general superintendence and directions of the affairs of the Authority."* The Chairperson can also exercise powers and "*do all such acts and things which may be exercised or done by the Authority under the Act."* In its current form the section does not include a clear provision for the senior leadership of the DPA to advice and participate with the Chairperson in the decision-making processes of the DPA. Moreover, the power of the Chairperson to act on behalf of the DPA appears to be very wide and not subject to review by a broader set of members. This raises concerns about the lack of accountability and transparency in the decision-making of the Chairperson. It is therefore submitted:

Sl. No.	Section No.	Page No.	Comment
			(i) the language of the draft Bill should reflect that the Chairperson together with the senior leadership and heads of internal departments are in-charge of the day to day operations of the DPA; (ii) matters which require the Chairperson to consult with the Board should be clearly identified and set out in the terms of reference of the Board; and (iii) the functions of the Chairperson should include approaching the Board to: • *"receive approval for set up and organisational structure of the DPA (and any significant changes thereto);* • *receive approval of annual reports and audits presented to the Board;* • *table reports on enforcement actions of the DPA; and* • *any other matters which the chairperson or any member of the board, with the approval of the chairperson, may refer for joint consideration of the Board."* (Dvara Research, 2018c). To reinforce internal accountability, the Chairperson should present the following to the Board: • *"its annual report on enforcement actions and complaints received;* • *statistics and reports from the Judicial Authority on disputes resolved; and* • *annual plans, budgets, audits and risk assessments."* (Dvara Research, 2018c).
57.	54	31	This section prevents the proceedings of the DPA from being held invalid due to "*(a) any vacancy or defect in the constitution of the Authority, (b) any defect in the appointment of a person as a chairperson or member; or, (c) any irregularity in the procedure of the Authority not affecting the merits of the case.*" This language has become standard in various legislations given the obstacles faced in practice by several state bodies. The motivation behind this section is appreciable. The functioning of an authority should not get disrupted due to vacancies within the authority. This is also a crucial learning from the design of the Cyber Appellate Tribunal, which was not empowered to preside over cases in the absence of its Chairperson.

Sl. No.	Section No.	Page No.	Comment
			Consequently, the Cyber Appellate Tribunal was not able to preside over any cases between March 2011 and April 2016 due to a prolonged vacancy in the office of the Chairperson. (Comptroller and Auditor General, 2016) However, it is submitted that the language in section 55 allows for the DPA to function despite wide discrepancies in its constitution and processes. For instance, Section 55(b) permits the DPA to continue its proceedings despite "*any defect in the appointment of a person as chairperson or member"*. This could potentially give rise to a situation where members with significant conflicts of interest are empowered to preside over the functioning of the DPA and such proceedings of the DPA could be upheld, given the existing drafting of the section. It is therefore recommended that the section should be redrafted in a manner that limits the scope of circumstances that would not render the proceedings of the DPA invalid.
58.	57	32	This section requires the Central Government to grant appropriate monetary dispensation to the DPA, for the purposes of the Act. Under this provision, the Central Government may dispense grants that it deems fit for the DPA to discharge its functions under the Act. It is submitted that the language in this provision should emphasise that the dispensation by the Central Government should be made compulsory and sufficient for the DPA to discharge its various functions. Some existing legislations clearly articulate the expenses that the grant by the Central Government must cover. (i) For instance, section 21 of the TRAI Act (1997) requires the Central government after due appropriation made by the Parliament, to "*make to the Authority grants of such sums and money as are required to pay salaries and allowances payable to the Chairperson and the members and the administrative expenses including salaries, allowances, and pension payable to or in respect of officers of other employees of the Authority."* The language in this provision sets out the expense heads that should be covered by the Central Government's grant and therefore, provides an indication of the quantum of the grant that should be made to the relevant authority.

Sl. No.	Section No.	Page No.	Comment
			(ii) Similarly the RTI Act 2005, requires the Central Government to provide the *"the Chief Information Commissioner and the information Commissioners with such officers and employees as may be necessary for the efficient performance of their functions under this Act, and the salaries and allowances payable to and the terms and conditions of service of the officers and other employees appointed for the purpose of this Act shall be such as may be prescribed."* This provision ensures that the office of the Chief Information Commissioner is equipped with sufficient capacity to discharge their functions. It is therefore submitted that drafting in this section should be reviewed to incorporate language that sets out the expense heads that should necessarily be covered by the grant of the Central Government, such as administrative expenses and the cost of personnel deployed by the DPA.
59.	59	32	This section sets out the reports that the DPA should present to the Central Government. Under this section, the DPA is required to furnish to the Central Government (i) *"returns and statements and such particulars in regard to any proposed or existing programme for the promotion and development of personal data"*, as the Central Government may require from time to time, and (ii) "*an annual report giving a summary of its activities during the previous year".* It is recommended that in addition to the above, (i) the DPA should include reporting *"on enforcement actions undertaken and complaints acted upon"* (Dvara Research, 2018c), in the annual report submitted to the Central Government, for summarising its activities of the previous year. (ii) *"the format for this report must be consistent across years, including such qualitative commentary as it sees fit*" (Dvara Research, 2018c). By furnishing these reports to the Central Government, the DPA will open itself to legislative scrutiny. Such a scrutiny is an important mechanism to hold the DPA accountable for the exercise of the powers vested in it.

Sl. No.	Section No.	Page No.	Comment
60.	60	33	This section sets out the different powers and functions of the DPA. The section compiles all functions that the DPA is expected to perform for the effective enforcement of the data protection regime as envisaged in the draft Bill. Some functions of the DPA include specifying circumstances where a DPIA may be required, hosting database of significant data fiduciaries along with data trust score provided to them on its website, providing a detailed criterion for assigning data trust score by data auditors, and maintaining a database of certification of significant data fiduciaries which is updated to reflect their modification, withdrawal, suspension or cancellation of certificates. It is submitted that: (i) the DPA should also perform the function of maintaining a database of all consumer complaints and enquiries received by the DPA. As emphasised in response to section 49(4) above, the DPA should provide for grievance redress at both zonal and central level. Therefore, the complaints received at both zonal and central offices of DPA should be logged into the centralised database; (ii) the centralised database should contain anonymized, case level information about the complaints received, and it should be open to public. (Dvara Research, 2018c). This database could provide actionable intelligence to the DPA for informing its enforcement actions; and (iii) the DPA should also encourage research on this database, which *"could generate policy insights and reveal vulnerabilities in the system, enabling a regulator to address them before they manifest in harms."* (Dvara Research, 2018c). Regulators in other jurisdictions have found the analysis of the complaints database in understanding the practices and behaviour of the regulated entities and the emerging trends in the market. The US Consumer Financial Protection Bureau (CFPB) analyses its complaints database to identify surges in specific complaint types; patterns across geographic areas, companies, and consumer demographics. It also enables them to look for consumer protection issues emerging in new products. They use these insights to prioritise their supervision and enforcement functions, often

Sl. No.	Section No.	Page No.	Comment
			allowing them to detect and address minor issues before they aggravate and become major problems. (Consumer Finance Protection Bureau, 2017).
61.	61	35	This section sets out provisions in relation to which the DPA can issue its own codes of practice or approve the codes of practice submitted by industry or trade associations after undertaking consultations with relevant sectoral regulators and stakeholders. The DPA is empowered to issue codes of practice in relation to several sections of the draft Bill. From a consumer protection perspective, this structure is a concern given that some substantive provisions do not contain enough clarity on policy and principle for the guidance of the provisions, but instead leave these to evolve from non-binding soft law codes of practice. For instance, clause (i) in sub-section 60(6) empowers the DPA to issue codes of conduct in relation to "*the exercise of any right by data principals under Chapter VI (Rights of Data Principals) of this Act."* This clause does not provide sufficient clarity on the purpose of the code of conduct. The relevant chapter also does not contain guidance on the levels of protection that the codes of practice should aspire for. This is matter of concern as codes are developed to encourage "*particular kinds of outcome*" (Parker, 2010). In addition to this, section 61(2) allows industry or trade associations, interest groups of data principals, sectoral regulators or statutory authorities or any department of ministries of the Central or the State Government to issue their own codes of conduct, thus activating co-regulation. While co-regulation allows flexibility to the regulated entities, the component of self-regulation is susceptible to such standards of adherence being proposed that are in the larger interest of particular interest groups or powerful stakeholders in the industry (Dvara Research, 2018a). Co-regulatory approaches also lead to a 'check-box' based compliance with a view to minimise regulatory burden, as has been the experience in other countries (McGeveran, 2016). We raise a concern to this regulatory approach, and it is suggested that the provision be extended to address the context and interests of every sector.

Sl. No.	Section No.	Page No.	Comment
62.	62	36	This section empowers the DPA to issue legally binding directions to data fiduciaries or data processors in general or to issue directions to any specific data fiduciary or data processor. Before issuing the direction, the DPA is required to provide a reasonable opportunity of being heard, to the relevant data fiduciary or data processor. The DPA can also modify or withdraw or suspend its directions and subject the modifications or suspensions to the imposition of conditions it may find appropriate. The final report of the Committee of Experts envisages the DPA to use a range of enforcement tools, embedded in the paradigm of responsive regulation to encourage compliance with the data protection regime. Accordingly, this Chapter deliberates a range of enforcement tools that could aid the DPA's enforcement actions. These include issuing or approving *"Codes of Practice"* (Section 61), the power of the DPA to *"issue directions"* (Section 62), *"call for information"* (Section 63), as well as the power to *"conduct inquiry"* (Section 64). The DPA is empowered to undertake any of these enforcement actions, in addition to a range of others such as issuing warning, issuing reprimand or suspending the processing activity of the defaulting entity. Evidently these enforcement actions vary in their punitive effects. The theory of responsive regulation requires a regulator to gradually escalate through these enforcement actions, beginning with the least punitive measures. The objective of responsive regulation is to ensure a dynamic, context sensitive and proportionate response to the contraventions of the defaulting entity (Dvara Research, 2018a). Consequently, the regulator needs to develop rules that guide the use of wide range of enforcement tools in order to ensure that the regulatory response is proportionate. The draft Bill contemplates the use of these enforcement tools by the DPA, however does not contain rules that can guide the DPA's regulatory escalation. Specifically, this section does not address: (i) the circumstances that can lead the DPA to consider issuing directions; and (ii) the extent of punitive nature of the direction. By not clearly articulating the principles and criteria on the basis of which the DPA can issue directions and escalate up to more punitive directions, the draft Bill has compromised on a necessary element of the paradigm

Sl. No.	Section No.	Page No.	Comment
			of responsive regulation. The public communication of the level and escalation of regulatory measures play an important role in signalling to the market that there are still high costs of non-compliance (Greenleaf, 2014) (Raghavan, 2018). This also complements the underlying game theoretic tenet of responsive regulation, that a credible threat of an ultimate, serious and costly regulatory imposition can encourage regulated entities to early on comply with the softer enforcement actions. A set of well-articulated principles for regulatory escalation will signal the willingness of the DPA to escalate to higher punitive actions when warranted. This will establish the DPA's legitimacy and set out a due process for exercising its enforcement power, which could encourage compliance with its softer enforcement actions. Compliance with law is more likely *"when regulation is seen as more legitimate and more procedurally fair"* (Braithwaite, 2011). The inclusion of such provisions will also guide the DPA in using its enforcement powers proportionately. Similar provisions are also recommended elsewhere, for instance the report of the Financial Sector Legislative Reforms Commission that sets out 11 principles to guide the proposed regulator in the use of its powers. The first principle emphasises that the regulatory action should be proportionate to the risk held by the regulated entity as well as the level of detriment caused by the regulated entity by not fulfilling its obligations (Financial Sector Legislative Reforms Commission, 2013). These principles to guide the use of powers of the DPA can act as the barometer against which the conduct of the DPA can be assessed; thus, acting as a lever for holding the DPA accountable in the use of its powers. *"Effective regulation requires effective accountability. If the control mechanism of accountability fails, then effective regulation is endangered, risking arbitrary exercise of regulatory power, inequity and loss of confidence in the regulatory system."* (House of Lords, Parliament of the United Kingdom, 2004) It is therefore submitted that: (i) the circumstances that can lead to the issuance of a direction should be clearly articulated in the draft Bill. This will help in ensuring transparency and consistency in the enforcement actions of the DPA,

Sl. No.	Section No.	Page No.	Comment
			(ii) the DPA should be empowered to initiate enforcement actions, including issuing directions (a) on its own initiative and based on referrals from other public authorities or government agencies. (b) The DPA should also be empowered to initiate enforcement actions "*on the basis of complaints, including on the basis of information received from the scrutiny of the complaints database* (as proposed in response to section 60)" where such information provides *"reasonable cause to suspect contravention, or the likelihood of contravention, of any provisions"* of the data protection regime (Dvara Research, 2018b), and (iii) the paradigm of responsive regulation, which has also been alluded to in the Report, requires that enforcement actions undertaken by a regulator should be proportionate and sensitive to the nature of the contravention. When deciding on the content of the Direction, the DPA should consider, "*the amount of unfair advantage as a result of such contravention, the amount of harm to any individual, and the repetitive nature of the default"* (Dvara Research, 2018b).
Chapter XI: Penalties and Remedies			
63.	69	42	Section 69(1) and 69(2) lay down the list of contraventions for which a data fiduciary is liable to be subject to a penalty and the amount of the penalty that is to be charged. The draft Bill specifies that a delinquent data fiduciary has to pay the higher of the amounts between, a penalty amount specified (5 or 15 crores for section 69(1) and 69(2) respectively) or a percentage of the "total worldwide turnover" (2 percent or 4 percent for section 69(1) and 69(2) respectively). Explanation (1) and (2) to Section 69 provides a description of the *"total worldwide turnover"* as used in sections 69(1) and 69(2). It is submitted that the use of "Explanations" in this provision is problematic, as the terms they include are in effect definitions required to apply the provision. Under principles of legislative drafting, an explanation to a section is not a substantive provision by itself (Sarathi, 2005). It is suggested that ambiguity in the provision is cleared by introducing the language contained in Explanation (1) & (2) as a definition in the substantive provision itself.

Sl. No.	Section No.	Page No.	Comment
64.	72	43	Section 72 specifies the penalty for the failure to comply with an order issued by the DPA. Differential penalties have been set out for data fiduciaries and data processors in the sub-section with data processors being subjected to significantly lower penalties. It has been earlier recommended in our submission (please refer to our comments on section 3(13) above) that all customer-facing entities should be treated as data fiduciaries given their direct and sensitive relationship with the data principals. Accordingly, it is also suggested that they are held to a higher standard of responsibility and are subjected to the higher standard of penalties.
65.	75(1) Explanation	44	Sub-section75(1) provides data principals with the right to seek compensation from a data fiduciary or a data processor. The explanation provided to section 75(1) specifies that a data processor will be liable to be approached for compensation only when, *"where it has acted outside or contrary to the instructions of the data fiduciary pursuant to section 37, or where the data processor is found to have acted in a negligent manner, or where the data processor has not incorporated adequate security safeguards under section 31, or where it has violated any provisions of this Act expressly applicable to it."* A digital service may have a network of data processors and multiple data fiduciaries. It is unreasonable to expect the data principal to understand this process and locate the precise point of failure when there is a violation which results in a harm to the data principal. To protect the data principals effectively, the system should be designed in a manner that allows the data principals to approach the user-facing entity, irrespective of the point of failure in the system. This provides further justification for the need for every customer-facing data processor to be classified as a data fiduciary (as recommended in our response on section 3(13)). It is also unfair and onerous to expect the data principal to look through arrangements between companies regarding data processing.

Sl. No.	Section No.	Page No.	Comment
			Accordingly, it is recommended that all (customer-facing) entities should be liable to provide compensation to the customers under the law. The arrangements and apportionment of liability amongst entities themselves should be a subject of their bilateral contractual arrangements, and not the burden of the data principal.
66.	75(2)	44	This sub-section allows a data principal to seek compensation pursuant to a complaint instituted in the prescribed form and manner. It is recommended that the procedure for seeking compensation should be standardised by the DPA in a manner which ensures that the process is accessible, timebound and fair for data principals. These principles may be realised in the following suggested ways: (i) The DPA may create a set of standardised forms (along with processes and evidentiary requirements) for compensation claims for different categories of violations. The standardisation in documentation will help facilitate further appeals processes and when a case is transferred to other Adjudicating officers and shall simplify the filing of the complaint for data principals. (ii) The Adjudicating officer should be free to additionally accept any compensation claim which is not captured in the formulation prescribed by the DPA. This shall ensure that data principals do not suffer on account of the differences in the format of the complaint. (iii) It is further recommended that the claim process is implemented through both offline and web-based complaint management systems. A web-based complaint management system (CMS) with the digital handling of documents and online tracking of compensation payments, can enable data principals to track their claims through its entire lifecycle and receive notifications and updates on cases. The presence of an offline complaints management system will ensure that the system does not raise barriers for those data principals who do not have access to the internet. Existing regulators such as SEBI offer similar complaint management processes, allowing customers to register complaints online as well as offline through the medium of physical letters, emails, or by personal visits to SEBI officers and are then uploaded online to

Sl. No.	Section No.	Page No.	Comment
			the centralized grievance redressal system (Task Force on Financial Redress Agency, 2016). The (CMS) system should also be able to publish its adjudication decisions and complaint related data analysis in multiple electronic formats as well as machine-readable format. While it is appreciated that resolution of complicated and large value disputes may require more time, a successful redress mechanism should use creative ways to respond to disputes as fast as possible (Task Force on Financial Redress Agency, 2016). The Task Force on Financial Redress Agency suggested that low value and simple complaints on financial harms are processed and resolved by a 2-week long fast-track process after they have been duly screened and accepted (Task Force on Financial Redress Agency, 2016). It is recommended, that the draft bill should deliberate similar provisions for handling smaller and complicated disputes separately. Resolution of smaller claims could be expedited. They could be processed and resolved in two weeks and all other complaints should be processed within a maximum of 180 days from a complaint being verified and accepted. Extensive digitization through the CMS (suggested above) could facilitate the timebound processing of complaints. (Task Force on Financial Redress Agency, 2016)
67.	77	45	Section 77 (*Data Protection Funds*) outlines the creation of two separate funds, (i) The Data Protection Authority Fund which is to receive all government grants, fees and charges and (ii) The Data Protection Awareness Fund which is to receive all sums realised by way of penalties and fines. It is observed that the creation of these two funds is an unusual exercise. ***Receipts of the DPA should be credited to the Consolidated Fund of India****:* Funds realised through receipts including penalties, fines and taxes are usually credited to the Consolidated Fund of India (See Constitution of India,1950 art. 266(1)). Important examples include authorities like the Competition Commission of India (see section 47 of the Competition Act) and SEBI that credit all penalties received to the Consolidated Fund of India (see section 15JA of Securities and Exchange Board of India Act, 1992). The broad regulatory principle involved here is that when fines are directly credited to an enforcement agency, there is a perverse incentive to over-regulate. Depending on grants from the consolidated fund of India also imparts a degree of parliamentary

Sl. No.	Section No.	Page No.	Comment
			supervision to the regulating authority, through the process of the Union Budget (Comptroller and Auditor General of India, 2008). Enforcement institutions in other countries also observe this principle. Penalties and fines collected by the US Federal Trade Commission (which enforces privacy rights in the US) are credited to the general fund in the U.S Treasury (once compensations to relevant affected principals has been paid) (Federal Trade Commission, 2017). It is therefore suggested that the DPA should be deriving its required monetary inflows solely from grants made by the government from the Consolidated Fund of India. ***Raising user awareness should not be conditional on the availability of funding through the Data Protection Awareness Fund**:* We appreciate the intention of the draft Bill to create a provision of separate funding for Data Protection Awareness. However, this function should not be subject to the availability of funds but a core function of the DPA. Given the need for educating data principals about the threats from online data processing, guidelines for keeping their data safe and their rights and remedies under this act, the DPA must take on a strong role to create such an awareness of a new regime. As also discussed in detail in our working paper, *"Effective Enforcement of a Data Protection Regime",* generating awareness about data protection is *"particularly relevant in the Indian context given that awareness about data protection remains low in the country and individuals do not fully understand the risks associated with sharing their personal data with other entitie"* (Dvara Research, 2018c). Other regulators such as the RBI are also actively focussing on generating awareness among consumers to address the challenges of consumer protection posed by limited financial awareness and literacy and the grave threat of financial risk to vulnerable customers. The RBI as a mature regulator has undertaken several steps to introduce financial literacy among a diverse group of Indians including measures such as setting up of Financial Literacy Centres; School Awareness Programs; and the introduction of financial literacy concepts in the school curriculum. These measures are informed by pan-India surveys conducted to measure the quality and extent of financial awareness in different population groups (Reserve Bank of India, 2016). Accordingly, we recommend that he DPA should perform functions to raise awareness of data protection. We propose that the DPA should actively design measures to:

Sl. No.	Section No.	Page No.	Comment
			(i) increase the public awareness around data protection particularly emphasising the need to protect personal data and the possibility of harms due to sharing personal data; (ii) generate awareness about the rights that data principals have been afforded under the law, the mechanism through which the rights can be exercised and the available redress mechanism; and (iii) engage constructively with data fiduciaries, data processors and various industry associations to proactively improve data protection practices in the country. Additionally, we suggest that the DPA also undertakes, (iv) pan-India surveys to assess awareness of data rights, risks of harms from data processing and redress mechanisms.
Chapter XIII: Offences			
68.	90, 91	51	These provisions create criminal offences whereby a person or group of persons are said to commit a crime where they "*knowingly or intentionally or recklessly*" act in contravention of the provisions of this Act resulting in: (i) significant harm to a data principal due to the obtaining, disclosing, transferring or selling or offering to sell personal data (section 90), and (ii) harm to a data principal due to the obtaining, disclosing, transferring or selling or offering to sell personal data (section 91). The punishment for causing significant harm from personal data (imprisonment up to 3 years or a fine up to rupees two lakh or both) is noticeably lower than the penalty for harm from sensitive personal data (imprisonment up to five years or a fine up to rupees three lakh or both).

Sl. No.	Section No.	Page No.	Comment
			Several concerns are raised from these provisions. (i) We refer you to our extensive comments in this submission on the definitions of "*harm*" and "*significant harm*" pointing out the flaws in the definition of the term and advising against its use as a determinative factor in other sections of the draft Bill. The poor conceptualisation of "*harm*" in this draft Bill make it a dangerous standard on which to predicate the creation of offences. It is a well settled rule of statutory interpretation that criminal or penal statutes must be strictly construed (Sarathi, 2005). This would be impossible if there is an inclusion of a vague or imprecise term such as *"harm"* or *"significant harm".* (ii) The quantum of punishments allotted for the mentioned offences appears to be based on a subjective value judgement that views the compromise of personal data as being less damaging for data principals unless "*significant harm*" is caused as a result. We reiterate our submission that these distinctions based on assessments of certain types of data being more harmful than others if compromised are erroneous in the modern world. The compromise of any personal data can result in harms of various magnitudes; this is dependent on the individual or entity accessing and/or processing the data itself, and not on the unnatural categorisation of the data into "sensitive" and "non-sensitive". In the era of big data, seemingly harmless, non-sensitive personal data can be recombined and aggregated to reveal protected, sensitive personal data (Ohm, 2010). (iii) We note with concern that the language in this section combines three different standards of criminal liability. Under its current formulation, offences are established on the basis that the accused parties acted "*knowingly or intentionally or recklessly*". First, each of these terms in our understanding attract different standards of liability as criminal law attributes higher liability for acts done with criminal intent, as compared to those committed with knowledge or due to negligence (Pillai, 2000) (*Jai Prakash vs. State (Delhi Administration) 1991 SCR (1) 202*). In addition, we note that the threshold of *recklessness* does not appear to be common in Indian jurisprudence; '*negligence'* and *'rashness'* are the most equivalent terms to *recklessness* found in Indian jurisprudence (Pillai, 2000). Considering that the three

Sl. No.	Section No.	Page No.	Comment
			standards attract different levels of penalties, combining them to create a single standard of liability as per sections 90 and 91 is problematic. Accordingly, we strongly recommend that these sections of the draft Bill be revisited and entirely re-constructed.
69.	92	52	Section 92 creates a criminal offence for "*re-identification and processing of de-identified personal data*". Such person is exempted if they can prove that the personal data in question "***belongs to***" them or the data principal to whom this personal data belongs to has consented for such re-identification. Section 92(1) appears to exempt data fiduciaries and/or data processors from obtaining consent for re-identification of personal data from the concerned data principals where the personal data is obtained from another data fiduciary or processor (i.e. not collected directly from a data principal). In effect, the provision only requires consent from the entity that shares the personal data rather than from the data principals whose data is being shared. (i) ***No restriction on sharing personal data without consent of the data principals***: The drafting of this provision is in alignment with the scheme of this draft Bill. Under the current scheme of the draft Bill, data fiduciaries are permitted to undertake a plethora of actions (under the definition of processing as per sub-section 3(32)) including *"alignment or combination"*, *"indexing"*, *"disclosure by transmission"* and "*making available [data]"* amongst several others. Accordingly, any impromptu transfers of data by the data fiduciary to a third party, and the processing actions they undertake subsequently (in this case, re-identification) would be deemed legal. As per sub-section 8(1)(g), information of such impromptu transfers of data must be provided to the concerned data principal "*as soon as is reasonably practicable"* in the form of a notice. It is submitted that the existing provisions give the data fiduciary or data processor seemingly unprecedented powers to share data with other parties without significant checks on such sharing. Therefore, we strongly recommend that the

Sl. No.	Section No.	Page No.	Comment
			structure of this provision be reconsidered to provide the data principal with more autonomy over their personal data as is an objective in the Preamble of this draft Bill. (ii) ***Personal data does not "belong" to data fiduciaries after collection:*** The language in this provision seems to indicate that entities that collect and share personal data "own" such personal data. Personal data does not fit the construct of property as has been recognised by many scholars, for several reasons including its fundamental inalienability, the difficulty in divesting interests in personal data and the enduring consequences that data principals suffer from the lack of data quality (Baron, 2012).In India, privacy and data protection are firmly in the realm of human rights following the *Puttaswamy* decision and therefore, personal data cannot be treated like property. Accordingly, we strongly recommend that these sections of the draft Bill be revisited and reviewed.
70.	95	52	A definition of "company" has been specified for the purpose of this section as an explanation to sub-section 95(3). It is submitted that the use of "Explanations" in this provision is problematic, as the terms they include are in effect definitions required to apply the provision. Under principles of legislative drafting, an explanation to a section is not a substantive provision by itself (Sarathi, 2005). It is suggested that ambiguity in the provision is cleared by introducing the language contained in the explanation as a definition in the substantive provision itself.
71.	96	53	This section places personal responsibility on officials occupying specified positions in State institutions when offences are committed. It also provides that such officials can be exempted from a penalty if they can prove that the offence was committed without their knowledge or that they had exercised all due diligence to prevent the commission of such an offence. Section 110 of the draft Bill provides an overriding effect over existing laws and instruments to ensure full compliance with the draft Bill and to ensure that the draft Bill prevails over any contradictory laws. In our

Sl. No.	Section No.	Page No.	Comment
			reading, this results in a loss of immunity or non-exemption from liability to such government officials or members of the armed forces that may act in contravention with the provisions of this draft Bill to discharge their official duties, as are afforded to such officials in Code of Criminal Procedure, 1973 (Section 45[3], 197(2)[4]) and Indian Penal Code, 1860 (Section 76[5], 78[6]). It would be helpful to have this clarified in the construction of this section to clarify the levels of immunity (if any) that government bodies or the employees enjoy under the draft Bill.

[3] Section 45 of the Code of Criminal Procedure, 1973.
"Protection of members of the Armed Forces from arrest.
(1) Notwithstanding anything contained in sections 41 to 44 (both inclusive), no member of the Armed Forces of the Union shall be arrested for anything done or purported to be done by him in the discharge of his official duties except after obtaining the consent of the Central Government.
(2) The State Government may, by notification, direct that the provisions of sub- section (1) shall apply to such class or category of the members of the Force charged with the maintenance of public order as may be specified therein, wherever they may be serving, and thereupon the provisions of that sub- section shall apply as if for the expression" Central Government" occurring therein, the expression" State Government" were substituted."
[4] *Section 197 of the Code of Criminal Procedure, 1973.*
"Prosecution of Judges and public servants.
No Court shall take cognizance of any offence alleged to have been committed by any member of the Armed Forces of the Union while acting or purporting to act in the discharge of his official duty, except with the previous sanction of the Central Government."
[5] *Section 76 of the Indian Penal Code, 1860.*
"Act done by a person bound, or by mistake of fact believing himself bound, by law.
Nothing is an offence which is done by a person who is, or who by reason of a mistake of fact and not by reason of a mistake of law in good faith believes himself to be, bound by law to do it. Illustrations
(a) A, a soldier, fires on a mob by the order of his superior officer, in conformity with the commands of the law. A has committed no offence.
(b) A, an officer of a Court of Justice, being ordered by that Court to arrest Y, and, after due enquiry, believing Z to be Y, arrests Z. A has committed no offence."
[6] Section 78 of the Indian Penal Code, 1860.
"Act done pursuant to the judgment or order of Court.
Nothing which is done in pursuance of, or which is warranted by the judgment or order of, a Court of Justice; if done whilst such judgment or order remains in force, is an offence, notwithstanding the Court may have had no jurisdiction to pass such judgment or order, provided the person doing the act in good faith believes that the Court had such jurisdiction."

SECTION III: BIBLIOGRAPHY

ACAS. (n.a.). *GDPR - The General Data Protection Regulation*. Retrieved from Advisory, Conciliation and Arbitration Service: http://www.acas.org.uk/index.aspx?articleid=3717#applygdpr

Advogados, L. (2017, December). *Data Protected - Brazil*. Retrieved from Linklaters: https://www.linklaters.com/en/insights/data-protected/data-protected---brazil

Al-Azizy, D., Millard, D., Symeonidis, I., Keiron, O., & Shadbolt, N. (2015). A Literation Survey and Classifications of Data Deanonymisation. *International Conference on Risks and Security of Internet and Systems* (pp. 36-51). Mytilene, Greece: Springer Internation Publishing. Retrieved August 23, 2018, from https://www.esat.kuleuven.be/cosic/publications/article-2576.pdf

Article 29 Data Protection Working Party. (2007). *Opinion 4/2007 on the concept of personal data.* Retrieved September 24, 2018, from http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf

ASSOCHAM India. (2014, May 7). *ASSOCHAM News*. Retrieved from ASSOCHAM India: http://www.assocham.org/newsdetail.php?id=4489

Awasthi, R. (2017, October 2017). To Save 'Make in India', Fix GST for Small and Medium Businesses. *The Wire*. Retrieved September 4th, 2018, from https://thewire.in/business/make-in-india-gst-sme

Barendt, E. (2016). Problems with the reasonable expectations of privacy test. *Journal of Media Law*, 129-137. Retrieved September 17, 2018, from https://www.tandfonline.com/doi/abs/10.1080/17577632.2016.1209326?src=recsys&journalCode=rjml20

Barocas, S., & Selbst, A. D. (2016). Big Data's Disparate Impact. *California Law Review*, 671-732. Retrieved September 17, 2018, from http://www.californialawreview.org/wp-content/uploads/2016/06/2Barocas-Selbst.pdf

Baron, J. B. (2012). *Property as Control: The Case of Information.* Retrieved September 15, 2018, from http://repository.law.umich.edu/cgi/viewcontent.cgi?article=1017&context=mttlr.

Birks, P. (2014). Lionel Cohen Lecture: The Content of Fiduciary Obligation. *Israel Law Review*, pp. 3-38. Retrieved September 24, 2018, from https://www.cambridge.org/core/journals/israel-law-review/article/lionel-cohen-lecture-the-content-of-fiduciary-obligation/201FD8938046C00314B2C83B05C823CB

Bombay Stock Exchange. (2018, September 20). *Complaints against Companies and Trading Members*. Retrieved from Bombay Stock Exchange: https://www.bseindia.com/investors/cac_tm.aspx?expandable=2

Braithwaite, J. (2011). The Essence of Responsive Regulation. *UBC Law Review*, 475-520. Retrieved 20 September, 2018, from http://johnbraithwaite.com/wp-content/uploads/2016/03/essence_responsive_regulation.pdf

Canadian Internet Policy and Public Interest Clinic. (2008). *Submission to the Personal Information Protection and Electronic Documents Act.* Retrieved September 17, 2018, from https://cippic.ca/sites/default/files/CIPPIC_PIPEDAsubm_15Jan08.pdf

Cavoukian, A. (2011). *Privacy by Design:The 7 Foundational Principles.* Retrieved from Information and Privacy Comission of Ontatrio.

CGAP, Dalberg & Dvara Research. (2017, November 16). *Privacy on the Line.* Retrieved September 14, 2018, from Dvara Research: https://www.dvara.com/blog/2017/11/16/privacy-on-the-line-what-do-indians-think-about-privacy-data-protection/

Charter of Fundamental Rights of the European Union. (2000, December). Retrieved September 17, 2018, from http://www.europarl.europa.eu/charter/pdf/text_en.pdf

Chik, W. B. (2013). The Singapore Personal Data Protection Act and an assessment of future trends in data privacy. *Computer Law and Security Review*, 554-575. Retrieved September 24, 2018, from https://ink.library.smu.edu.sg/cgi/viewcontent.cgi?article=3204&context=sol_research

Chugh, B., & Raghavan, M. (2017, October 3). Moving Towards a User Data Regime. *Livemint*. Retrieved September 24, 2018, from https://www.livemint.com/Opinion/6bNi3LnWTH2JWEpZmSuuBI/Moving-towards-a-user-data-rights-regime.html

Committee of Experts on A Data Protection Framework for India. (2018). *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians.* Ministry of Electronics and Information Technology, Government of India.

Committee on Reforms of Criminal Justice System. (2003, March). Committee on Reforms of Criminal Justice System. Ministry of Home Affairs, Government of India. Retrieved September 5, 2018, from https://mha.gov.in/sites/default/files/criminal_justice_system.pdf

Comptroller and Auditor General. (2016). *Report of the Comptroller and Auditor General for year ended March 2015 (No. 29 of 2016).* Retrieved 20 September, 2018, from https://cag.gov.in/sites/default/files/audit_report_files/Union_Communication_IT_Compliance_Report_29_2016.pdf

Comptroller and Auditor General of India. (2008). *Report No.CA 1 of 2008.* Retrieved September 24, 2018, from Comptroller and Auditor General of India: https://cag.gov.in/sites/default/files/old_reports/union/union_compliance/2007_2008/Civil/Report_no_1/chap_6.pdf

Consumer Finance Protection Bureau. (2017). *Consumer Response Annual Report 2016.* Retrieved September 20, 2018, from https://files.consumerfinance.gov/f/documents/201703_cfpb_Consumer-Response-Annual-Report-2016.PDF

DiGangi, C. (2018, September 21). *What is a Schumer Box?* Retrieved from Credit.com: https://www.credit.com/credit-law/what-is-a-schumer-box/

Directorate of Enforcement. (n.d.). *Organisational Chart of the Directorate of Enforcement*. Retrieved September 20, 2018, from Enforcement Directorate: http://www.enforcementdirectorate.gov.in/offices/organizational_chart.pdf#zoom=150?p1=1188201537437955901

Dvara Research. (2018a, February 7). *Responses dated 31 January 2018 to the "White Paper of the Committee of Experts on a Data Protection Framework for India" dated 27 November 2017 (White Paper) released by the Ministry of Electronics and Information Technology (MeitY).* Retrieved September 14, 2018, from Dvara Research: https://www.dvara.com/blog/wp-content/uploads/2018/02/Response-to-White-Paper-Public-Consultation-Dvara-Research.pdf

Dvara Research. (2018b, February 7). *The Data Protection Bill, 2018.* Retrieved from Dvara Research: https://www.dvara.com/blog/2018/02/07/our-response-to-the-white-paper-on-a-data-protection-framework-for-india/

Dvara Research. (2018c). *Effective Enforcement of a Data Protection Regime.* Retrieved September 20, 2018, from https://www.dvara.com/blog/wp-content/uploads/2018/07/Effective-Enforcement-of-a-Data-Protection-Regime.pdf

EU Directive 2016/680. (2016). DIRECTIVE (EU) 2016/680 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. Retrieved September 10, 2018, from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L0680&from=EN

EU Regulation 2016/679. (2016). Regulation 2016/679 of the European Parliament (General Data Protection Regulations). Retrieved September 10, 2018, from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN

European Data Protection Supervisor. (2017). *Assessing the necessity of measures that limit the fundamental right to protection of personal data: A toolkit.* European Data Protection Supervisor. Retrieved September 10, 2018, from https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf

European Data Protection Supervisor. (2018). *Guidelines on the Protection of Personal Data in IT Governance and IT Management of EU Institutions.* European Data Protection Supervisor. Retrieved September 17, 2018, from https://edps.europa.eu/sites/edp/files/publication/it_governance_management_en.pdf

Federal Trade Commission. (2012). *Protecting Consumer Privacy in an Era of Rapid Change.* Retrieved September 17, 2018, from https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf

Federal Trade Commission. (2017). *The Bureau of Consumer Protection Office of Claims and Refunds Annual Report 2017.* Retrieved September 19, 2018, from https://www.ftc.gov: https://www.ftc.gov/reports/bureau-consumer-protection-consumer-refunds-program-consumer-refunds-effected-july-2016-6

Federal Trade Commission Act. (2010). Retrieved September 24, 2018

Financial Sector Legislative Reforms Commission. (2013). *Report of the Financial Sector Legislative Reforms Commission: Volume I.* Retrieved September 20, 2018, from https://dea.gov.in/sites/default/files/fslrc_report_vol1_1.pdf

Grannis, m. (2015). You Didn't Even Notice! Elements of Effective Online Privacy Policies. *Fordham Urban Law Journal*, 1109-1166.

Group of Experts on Privacy. (2012). *Report of the Group of Expeerts on Privacy.* Retrieved September 24, 2018, from http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf

HM Treasury and Cabinet Office, Government of United Kingdom. (2017). *Corporate Governance in Central Government Department.* Retrieved September 20, 2018, from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/609903/PU2077_code_of_practice_2017.pdf

House of Lords, Parliament of the United Kingdom. (2004). *The Regulatory State: Ensuring its Accountability, Volume I.* Retrieved September 20, 2018, from https://publications.parliament.uk/pa/ld200304/ldselect/ldconst/68/68.pdf

Hustinx, P. (2010, August). Privacy by design: delivering the promises. *Identity in the Information Society*, 253–255. Retrieved September 17, 2018, from https://link.springer.com/content/pdf/10.1007/s12394-010-0061-z.pdf

ICDPPC. (2010). Resolution of Privacy by Design. Jerusalem. Retrieved September 18, 2018, from https://icdppc.org/wp-content/uploads/2015/02/32-Conference-Israel-resolution-on-Privacy-by-Design.pdf

IEEE. (2016). *Personal Data and Individual Access Control.* Retrieved September 21, 2018, from https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/other/ead_personal_data_v2.pdf

Information Commissioner's Office. (2018, September 24). *Principle (a): Lawfulness, fairness and transparency*. Retrieved from UK Information Commissioner's Office: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/

ITU-infoDev. (2018, September 17). *Elements of an Effective Regulator*. Retrieved from ICT Regulation Toolkit: http://www.ictregulationtoolkit.org/toolkit/6.5

Jethmalani, H. (2017, May 4). GST: Rising cost of compliance to hurt SMEs the most. *Live Mint*. Retrieved September 4, 2018, from https://www.livemint.com/Money/otQgEfXPUmGoPVB0rWinJK/GST-Rising-cost-of-compliance-to-hurt-SMEs-the-most.html

Justice K.S. Puttaswamy(Retd.) v. Union of India, Writ Petition (Civil) No. 494 of 2012 (Supreme Court of India August 24, 2017). Retrieved September 17, 2018, from https://www.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf

Maneka Gandhi vs Union Of India, 1978 SCR (2) 621 (Supreme Court of India January 25, 1978). Retrieved September 24, 2018, from https://www.sci.gov.in/jonew/judis/5154.pdf

Martin, K. (2015). Privacy Notices as Tabula Rasa: An Empirical Investigation into How Complying with a Privacy Notice Is Related to Meeting Privacy Expectations Online. *Journal of Public Policy and Marketing*, 210-227. Retrieved September 17, 2018, from http://journals.ama.org/doi/10.1509/jppm.14.139?code=amma-site

Mathiharan, K. (2014). Law on Consent and Confidentiality in India: A need for clarity. *National Medical Journal of India*, 39-42. Retrieved August 23, 2018, from http://archive.nmji.in/archives/Volume-27/Issue-1/27-1-SFM-III.pdf

McGeveran, W. (2016, August 5). *Friending the Privacy Regulators.* Retrieved September 24, 2018, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2820683

Miller, P. B. (2011). A Theory of Fiduciary Liability. *McGill Law Journal*, pp. 235-288. Retrieved September 24, 2018, from https://www.erudit.org/en/journals/mlj/2011-v56-n2-mlj1517315/1002367ar/

Ministry of Electronics and Information Technology. (2018, September 5). *Press Release on Feedback on Personal Data Protection Bill.* Retrieved September 24, 2018, from Ministry of Electronics and Information Technology: http://meity.gov.in/writereaddata/files/PDPB_feedback.pdf

Ministry of Human Resource Development, Government of India. (2011). *Statistics* . Retrieved from Ministry of Human Resource Development, Government of India: http://mhrd.gov.in/sites/upload_files/mhrd/files/statistics/Population2011.pdf

Narayanan, A., & Shmatikov, V. (2008). Robust De-anonymisation of large datasets. *2008 IEEE Symposium on Security and Privacy* (pp. 111-125). Washington DC: IEEE Computer Society. Retrieved August 23, 2018, from https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf

Nissenbaum, H. (2004). Privacy as Contectual Integrity. *Washington Law Review*.

OECD. (2013). *Principles for the Governance of Regulators.* Retrieved September 20, 2018, from http://www.oecd.org/gov/regulatory-policy/Governance%20of%20Regulators%20FN%202.docx

Office of the Australian Information Commissioner. (2018). *Australian Privacy Principles guidelines.* Retrieved September 4, 2018, from https://www.oaic.gov.au/resources/agencies-and-organisations/app-guidelines/APP_guidelines_complete_version_2_March_2018.pdf

Office of the Registrar General & Census Commissioner of India. (2015). *Table C8, Census of India 2011.* Retrieved September 24, 2018, from http://www.censusindia.gov.in/2011census/C-series/C08.html

Ohm, P. (2010). Broken Promises of Privacy: Responding to the Surprising Failure of Anonymisation. *UCLA Law Review*, 1701-1777. Retrieved September 15, 2018, from https://www.uclalawreview.org/pdf/57-6-3.pdf

Parker, M. H. (2010). Normative Lessons: Codes of Conduct, Self-regulation and the law. *The Medical Journal of Australia*, 658-660. Retrieved September 20, 2018, from https://www.mja.com.au/system/files/issues/192_11_070610/par10068_fm.pdf

Pillai, P. A. (2000). *Criminal Law* (9th ed.). New Delhi: Butterworths India.

Prins, C. (2006). Property and Privacy: European Perspectives and the Commodification of Our Identity. *Information Law Series*, 223-257. Retrieved September 15, 2018, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=929668

(2012). *Privacy Ammendment (Enhancing Privacy Protection) Act.* Retrieved September 21, 2018, from https://www.legislation.gov.au/Details/C2012A00197

(2013). *Protection of Personal Information Act of South Africa.* Retrieved September 21, 2018, from http://www.justice.gov.za/inforeg/docs/InfoRegSA-POPIA-act2013-004.pdf

Raghavan, M. (2018, January 11). Before the Horse Bolts. *Think Pragati*. Retrieved September 20, 2018, from https://www.thinkpragati.com/think/brainstorm/3180/before-the-horse-bolts/

Rao, G. S. (2003). *Special Contracts (Law of Contract-II).* Hyderabad: S. Gogia & Company.

RBI and Others v Jayantilal N Mistry and Others, TRANSFERRED CASE (CIVIL) NO. 91 OF 2015 (Supreme Court of India December 16, 2015). Retrieved September 27, 2018, from https://www.sci.gov.in/jonew/judis/43192.pdf

Reserve Bank of India. (2006). The Banking Ombusman Scheme. Mumbai. Retrieved from https://rbidocs.rbi.org.in/rdocs/Content/PDFs/BOS2006_2302017.pdf

Reserve Bank of India. (2014, May 14). *Notification on Opening of Bank Accounts in the name of Minors*. Retrieved from Reserve Bank of India: https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=8872&Mode=0

Reserve Bank of India. (2016). *Cyber Security Framework in Banks.* Retrieved September 17, 2018, from https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NT41893F697BC1D57443BB76AFC7AB56272EB.PDF

Reserve Bank of India. (2016). *Report on Trend and Progress of Banking in India 2015-16.* Retrieved September 19, 2018, from https://rbidocs.rbi.org.in/rdocs/Publications/PDFs/0FRTP16A120A29D260148E58B484D4A60E381BB.PDF

Sarathi, V. P. (2005). *Interpretation of Statutes.* Eastern Book Company.

Sébastien Gambs, M.-O. K. (2014). De-anonymization attack on geolocated data. *Journal of Computer and System Sciences, Elsevier*, 1596-1614. Retrieved August 23, 2018, from https://hal.archives-ouvertes.fr/hal-01242268/document

Shaw, T. (2017, January 24). *What skills should your DPO absolutely have?* Retrieved September 17, 2018, from The International Association of Privacy Professionals: https://iapp.org/news/a/what-skills-should-your-dpo-absolutely-have/

Shukla, V. (2003). *Constitution of India.* New Delhi: Eastern Book Company.

Sinha, M. (2018, June 18). Demo & GST: Empirical evidence shows MSMEs yet to recover from the twin economic measures. *Economic Times*. Retrieved September 17, 2018, from https://economictimes.indiatimes.com/small-biz/sme-sector/demo-gst-empirical-evidence-shows-msmes-yet-to-recover-from-the-twin-economic-measures/articleshow/64629419.cms

Solove, D. J. (2012). *Privacy Self-Management and the Consent Dilemma*. Retrieved September 14, 2018, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2171018

Solove, D. J., & Citron, D. K. (2016). *Risk and Anxiety: A Theory of Data Breach Harms.* 96 Texas Law Review 737 (2018); GWU Law School Public Law Research Paper No. 2017-2; GWU Legal Studies Research Paper No. 2017-2;. Retrieved August 31, 2018, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2885638

Task Force on Financial Redress Agency. (2016, June 30). *Report of the Task Force on Financial Redress Agency.* New Delhi. Retrieved September 19, 2018, from https://dea.gov.in/sites/default/files/Report_TaskForce_FRA_26122016.pdf

The Data Protection Bill of Kenya. (2018). Retrieved September 17, 2018, from http://www.parliament.go.ke/sites/default/files/2017-05/Data_Protection_Bill_2018.pdf

UNICEF. (2017). *Children in a Digital World.* UNICEF. Retrieved September 5, 2018, from https://www.unicef.org/publications/files/SOWC_2017_ENG_WEB.pdf

United Nations. (1985, November 29). Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power. Retrieved September 5, 2018, from http://www.un.org/documents/ga/res/40/a40r034.htm

University of California-Berkeley School of Law. (2008). *Security Breach Notification Laws:Views from Chief Security Officers.* California. Retrieved September 17, 2018, from https://www.law.berkeley.edu/files/cso_study.pdf

US Federal Communications Commission. (2016). *Comment of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission.* US Federal Communications Commission. Retrieved August 23, 2018, from https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-bureau-consumer-protection-federal-trade-commission-federal-communications-commission/160527fcccomment.pdf

US Federal Deposit Insurance Corporation. (2017). *Compliance Examination Manual: Evaluating Impact of Consumer Harm.* US Federal Deposit Insurance Corporation. Retrieved August 31, 2018, from https://www.fdic.gov/regulations/compliance/manual/2/ii-2.1.pdf

World Bank. (2016). *How to Notes: Designing effective redress mechanisms for bank-financed projects.* Retrieved September 20, 2018, from http://siteresources.worldbank.org/EXTSOCIALDEVELOPMENT/Resources/244362-1193949504055/4348035-1298566783395/7755386-1301510956007/GRM-P1-Final.pdf

Yusoff, Z. M. (2011). The Malaysian Personal Data Protection Act 2010: A Legislation Note. *New Zealand Journal of Public and International Law*, 119-155.