Comments on the (Draft) Personal Data Protection Bill, 2018

Rishab Bailey, Vrinda Bhandari, Smriti Parsheera, Faiza Rahman

National Institute of Public Finance & Policy (NIPFP)*

10 October 2018

1 Overview

This response presents our comments on the Draft Personal Data Protection Bill, 2018 ("*Bill*") proposed by the Justice B.N. Srikrishna Committee of Experts ("*Srikrishna Committee*"). We find that the Bill offers a fairly comprehensive set of data protection principles and rights to data subjects, particularly in relation to data processing by private entities. However, for the reasons explained in more detail in the response below, the position adopted by the Bill on certain key issues needs to be revisited.

- The provisions pertaining to **cross border transfer of data** must be revisited, particularly in view of their overbroad nature, the limited privacy related benefits this would bring and the concomitant costs it may impose on expression and other rights.
- The **scope of exemptions granted to government agencies** for security and law enforcement purposes must be reviewed to bring the provisions in line with Supreme Court's judgments in *Puttaswamy v. Union of India (2017)* (right to privacy case) and *KS Puttaswamy v. Union of India (2018)* (Aadhaar case), and ensure an adequate balance between privacy rights of individuals and the needs of state security.

*Rishab Bailey, Smriti Parsheera and Faiza Rahman are technology policy researchers at NIPFP, New Delhi. Vrinda Bhandari is a practicing advocate in Delhi. We thank Devendra Damle for his inputs in the section on genetic data.

- The other **exemptions granted under Chapter IX of the Bill** also need to be revisited on several counts. This will include adding categories such as academic and artistic work, while making the extent of the existing exemptions more nuanced, thereby ensuring a more appropriate balance of privacy with competing rights such as the freedom of expression, right to profession, etc.

In addition, there is also a need for bringing about further clarity on several other grounds, including on the **definitions and scope of key terms** included in the Bill such as the words 'anonymised', 'harm', 'sensitive personal data', 'personal data breach', 'disclosure to the public' and 'genetic data'; the **scope of the obligations under Section 4** (pertaining to fair and reasonable processing); the **scope of the grounds for processing by the state** in exercising various functions, as mentioned in Sections 13 and 19 of the Bill; and **the data breach notification mechanisms** in the Bill, which amongst other shortcomings, does not envisage notice being mandatorily provided to individuals where their personal data has been accessed or used without authorisation.

When it comes to the **structure and processes of the Data Protection Authority** (*"DPA" or "Authority"*) we find that the Bill is in need of significant improvements. In terms of its composition, the DPA consists of a Chairperson and only whole-time members. There is merit in considering the inclusion of part-time, non-executive members on the DPA who can bring in the requisite expertise into the agency while also providing checks and balances against any management issues in the agency. We had also recommended in our response to the White Paper that adjudicating of individual complaints under the data protection law should be done by a body that is separate from the DPA (Bhandari, Rahman, Parsheera, Kak & Sane, 2018). The reasons for this are explained further in our response.

Further, the Bill does not mandate the DPA to **ensure transparency** in the discharge of all its functions, a provision that is necessary in such a law given the wide range of powers being conferred upon the DPA. Further, except in case of the codes of practice, the Bill does not lay down provisions for effective public participation in the DPA's regulation-making processes (Parsheera, 2018). We propose that the law should require the DPA to undertake an assessment of the expected costs and benefits of any proposed regulation and seek to adopt measures that minimise the compliance costs while meeting the intended objective. Equally, the law should also mandate the DPA to provide an explanation for the decision finally adopted by it and the broad reasons for acceptance or rejection of the comments raised by stakeholders and the public.

Finally, the broad criminalisation provisions in the law and their treatment as cognizable and non-bailable offences also raises several concerns, which are explained in the following section.

2 Chapter-wise comments

This section contains our comments on select sections of the Bill, arranged in chapter-wise form.

2.1 Applicability

The law as currently drafted applies data protection obligations only to the personal data of living individuals (Section 2 read with Section 3(29)). However, it may be useful to consider extending the scope of certain protections to personal data of the deceased, as well as that of unborn children.

First, there may be circumstances where personal data (and particularly genetic or biometric data) of the deceased can be used to glean information about living people. For instance, one may be able to determine the chances of a living person getting a particular disease based on study of a deceased relatives' tissues. In such circumstances, publishing information pertaining to even the deceased person may affect the privacy rights of the living. The law should therefore clarify and account for such situations.

Second, it may often be practically difficult to identify if a person is dead or alive, leading to the possibility of reduced protections for living individuals. This is an issue that the Article 29 Working Party has also noted (Article 29 Working Party, 2007).

Thirdly, the law may also consider the issue of whether a living person has rights to the personal data of the deceased - for instance, where relatives may want to access social media accounts or emails of a deceased individual.

Finally, the law may also need to clarify the position with respect to unborn children. Given the increasing use of methods such as test tube babies, IVF etc., it is entirely possible that publication of genetic and other sensitive personal data of an unborn child may cause harms to the child once born. One must also consider the cases of embryos and other genetic material that has been frozen and the effects that dissemination of information in this regard may have on the individual once born.

2.2 Definitions

Certain defined terms in the Bill need to be clarified in order to aid certainty and ensure uniformity in the application of the proposed law.

- **Section 3(3) - "anonymisation":** The current definition in the Bill indicates that anonymisation of data should be "irreversible" in nature and should meet the standards specified by the Authority. There is considerable literature that indicates that perfect anonymisation may be hard if not impossible to achieve (not least due to new recombination methods that are constantly developing). Therefore, the draft law possibly sets an unachievable standard for anonymisation by using the word "irreversible".[1]

  The Srikrishna Committee Report notes that "*a general standard in the definition of anonymisation regarding the possibility of identification, should be sufficient to guide the DPA...any absolute standard requiring the elimination of every risk including extremely remote risks of re-identification may be too high a barrier and may have the effect of minimal privacy gains at the cost of greater benefits from the use of such data sets.*" The European Article 29 Working Party has also acknowledged this issue in Article 29 Working Party (2007), arguing that anonymous data is that data which cannot be used to identify the individual despite taking *all reasonable means* to do so. The Working Party notes that a case-by-case analysis is required to see if any measures reasonably likely to be used, will result in the ability to identify a person.

  It may therefore be useful for the definition to clarify that data fiduciaries are required to meet the standard of anonymisation specified by the Authority. The Authority should in turn be required to ensure that the standards that it specifies incorporates the irreversible process of transforming personal data to a form that makes it reasonably impossible for it to lead to identification of an individual. A separate provision could be introduced detailing the other factors for the Authority to consider in setting the relevant standards and codes of practice on anonymisation.

- **Section 3(20) - "genetic data":** Genetic data is part of "sensitive personal data" under section 3(35) of the Bill. However, the Bill limits the scope of genetic data to genetic characteristics which "*give unique information about the behavioural characteristics, physiology or the health of that natural person*". This implies that the definition only covers coding DNA. However,

[1] Refer for instance to Narayanan and Shmatikov (2008), Gambs, Killijian and del Prado Cortez (2014), Anderson (2009) and Al-Azizy, Millard, Symeonidis, O'Hara and Shadbolt (2015).

a lot of the DNA in the genome does not in fact give any information about a person's behavioural characteristics, physiology or health. Such DNA, known as "non-coding DNA" can nonetheless be used for DNA profiling. DNA profiles in turn can be used for establishing a person's identity, as well as for establishing genealogy and kinship, for instance through paternity tests. Indeed, the most widely used protocols today specifically use non-coding DNA for profiling, precisely because it cannot yield any information besides identity and genealogy/ kinship (Hares, 2015). The United States national and state DNA databases for example use 13 loci (sequences of DNA at specific locations in the genome), known as CODIS loci. These have been selected specifically for their reliability in establishing identity without revealing any other information (National Research Council Committee on DNA Technology in Forensic Science, 1992). The Law Commission of India (2017), in its 271st report on a Bill for establishing a DNA databank, also stated that the 13 CODIS loci would be used for DNA profiling.

The DNA Technology (Use and Application) Regulation Bill, 2018, which is currently pending in the Lok Sabha, leaves this determination of determining the sequences to be used for DNA profiling to the DNA regulatory board. Based on the above discussion, we can expect that the DNA databanks under the DNA bill will are also likely to use these 13 CODIS loci. However, these DNA profiles will not be covered under the definition of "genetic data" under the provisions of the present Bill. This is because the definition does not include the entire gamut of DNA profile data within its ambit. To remedy this lacuna, the definition of "genetic data" must be expanded to include DNA profiles which can be used to establish identity, genealogy or kinship.

- **Section 3(21) - "harm":** The definition of 'harm' in Section 3(21) is important as it forms the trigger for various rights / obligations under the Bill. It is used in provisions relating to personal data breach notifications, data protection impact assessments, data audits, adjudication, compensation and determination of offences. In each of these cases the responsibility of determining the likelihood and severity of the harm lies upon the data fiduciary or officers of the DPA or officers investigating an offence. This adds an element of subjectivity to the law and absent any guidance in the law or regulations framed by the DPA on what could be regarded as harmful in particular contexts, it could lead to an overly restrictive or expansive reading of the corresponding provisions.

  For instance, in the harm of "discriminatory treatment" in Section 3(21)(vi), it is unclear what specifically amounts to discriminatory treatment or the standard to be applied in this regard. Would this bar the use of personal

data to charge differential prices for services or offer different services to different individuals? While such issues will clearly require jurisprudence to develop around them, it would be useful to have some standards/ tests to be applied by the different actors responsible for assessing harms in different contexts. For instance, an assessment of discrimination may involve applying the standards under Article 14 (arbitrariness) or Article 15 (protected grounds include sex, caste, etc) of the Constitution of India, but also require a broader set of standards on other possible types of discrimination. Requiring the DPA to offer some clarification around these issues will enable greater certainty in the interpretation / application of the provisions.

At the same time, the data protection law must also account for harms that may arise in the future, including through new technological innovations allowing the use of personal data in unforeseen ways. Limiting the scope of the harm caused therefore limits the remedies available to individuals. Situations that are not covered in the list of harms under the current provision incude:

1. Loss of confidentiality of personal data, including in situations where the personal data may be provided under specific professional settings. The mere fact that personal data is removed from the context in which it was provided / capable of being used in an unauthorised manner, can lead to a variety of harms to individuals - not least anxiety or psychological harm. As noted by Nissenbaum (2004), privacy can be seen as the ability of the individual to control the 'context' and 'flow' of personal information. By de-contextualisation of personal data - i.e. the use of personal data in contexts/situations not originally intended by the individual, privacy rights are affected.

   In addition, while professional confidentiality rules may cover certain instances (for instance, in a lawyer-client relationship or a doctor-patient), professional confidences must also be included in the general data protection law so as to ensure individuals are adequately protected and have relevant remedies in the event professional secrecy is breached.[2] Information provided in such relationships can be of an extremely sensitive nature and accordingly, such harms must also be protected under the proposed privacy law.

2. Possibility of psychological manipulation of individuals or the restric-

[2]While higher standards may be set by relevant professional organisations, the general data protection law must attempt to provide a minimum standard of protection to personal data across sectors.

tion of autonomy of an individual. We are only recently becoming aware of the way in which behavioural economics, artificial intelligence and big data can be used to predict and directly affect how people feel and behave. The Cambridge Analytica incident as well as numerous Facebook related experiments demonstrate the ease of using personal data to manipulate individuals (Rushe, 2014) and (Zhukova, 2017). Accordingly, such circumstances may also need to be included within the definition of harm, particularly in view of the fact that such harms may otherwise be difficult to demonstrate for an individual plaintiff.

One of the aims of privacy rights is to protect the autonomy of the individual and ensure the exercise of agency during decision making. Increasingly, personal data can be used, through a variety of data mining and analysis techniques, to manipulate an individual's decision making and behaviour. While this may not be problematic when at a trivial or small scale (say, in the context of videos being recommended based on past behaviour), or where consent is taken (including in the form of opt-outs), behaviour modification can be problematic when it comes to actions with non-trivial consequences - whether it is voting in elections or buying a product.

The law must therefore account for the possibility of harm being caused to individuals through behaviour modification, where such behaviour modification leads to non-trivial consequences on the individual.

3. The use of a 'reasonable expectation' test in sub-clause (x) also creates some concerns. First, this may open the door to normalise surveillance practices in society, which cannot be the intent of the law. For instance, we are increasingly seeing the use of CCTV in schools and other places of learning. Not only will this mean that children may grow up with an expectation of constant surveillance, it normalises the practice, which can be dangerous to society as a whole. This is particularly problematic in a country such as India where technological standards can very often be made de rigeur without sufficient public awareness or debate.[3]

   The provision as currently drafted allows data fiduciaries to claim that as notice of surveillance was provided / surveillance should be expected as a matter of course. This fails to consider that the harm of surveillance is not only due to the fact that scrutiny is unexpected, but in the behavioural and other changes associated with being constantly

[3]It has been noted that the test is both unpredictable and biased in its application towards the urban poor in the United States (Simmons, 2015).

watched/scrutinised (Galic, Timan & Koops, 2016). Irrespective of whether a person has an expectation of being surveilled or not, surveillance affects a persons behaviour and autonomy (Galic et al., 2016).

Second, the expectation of privacy test does not use consistent standards or methods of application. Even the United States Supreme Court has used a variety of approaches to apply this test – implying a lack of certainty and uniformity in application of law.[4] For an intrusion to be found reasonable, the expectation must be "both subjectively and objectively reasonable". Applying these standards to newer digital technology has proved difficult - leading to lowered privacy protections (Crowther, 2012).[5]

Third, as newer technology, with more capacity to invade privacy becomes ubiquitous, it is possible that the reasonable expectation of privacy test may prove meaningless (Schneier, 2009). While technology may make it easier to violate privacy, this does not imply that privacy *must* be violated. The normative position on privacy must be independant of the possible ubiquity of a technological solution (Schneier, 2009).

In this context, it may also be useful to refer to Solove (2006) which provides a taxonomy of privacy and the harms that result from violation of rights. Solove identifies 16 categories of privacy and harms - surveillance, interrogation, aggregation, identification, insecurity, secondary use, exclusion, breach of confidentiality, disclosure, exposure, increased accessibility, blackmail, appropriation, distortion, intrusion and decisional interference (Solove, 2006). While this is not a perfect or exhaustive list, the definition of 'harm' in the personal data protection law must be analysed against each of these cases to assess whether individual rights are being adequately protected against known harms.

These comments must be read with our later comments pertaining to the offences/penal provisions under the draft law. We do not suggest expanding the scope of criminal provisions, which may lead to the law being considered draconian. Instead, we recommend adoption of a risk based approach - offences should be graded based on the risk/probability of harm and the nature of the likely harm.

[4]Kerr (2007) and Kistner (2016).

[5]Crowther cites four main reasons for this inability of the test to cope with new digital technology - (i) the increased gap between subjective and objective expectations in digital contexts, (ii) contractual arrangements with Internet service providers, (iii) storage of information on third-party servers, and (iv) judges' technological inexperience (Crowther, 2012).

- **Section 3(35) - "sensitive personal data":** In addition to the list given under the provision, the law must be clear on whether data that can reasonably be used to determine or infer sensitive personal data is included within the definition of the phrase. Just as the definition of the term "personal data" includes within it all data that can be reasonably used to identify an individual, a similar standard should apply to sensitive personal data. Thus, all data that can, directly or indirectly, reveal any sensitive personal data should be included within the ambit of the term.

  Further, the definition of the term "sensitive personal data" must also contain scope for a context specific determination (of what constitutes sensitive data). In addition to specifying broad categories of sensitive data, one must consider that it may very often be the context of the processing that leads to a determination of whether the data is sensitive or not. For instance, treating location data as personal data may or may not be problematic as a general rule, but in certain contexts (such as communication surveillance) this data may require higher protection. By not allowing for the possibility of additional protections on information that can be used to infer sensitive personal data, the Bill, may in certain contexts, render the protections afforded to sensitive personal data meaningless.

  While the Srikrishna Committee Report notes that there may be a cost in permitting a contextual determination of what constitutes "sensitive personal data", this argument is unconvincing, given that the law does not hesitate to impose costs on entities in areas where the gains as far as privacy protections are concerned are not particularly clear (for instance, the provisions pertaining to localisation/ mirroring of data). As noted in the Report itself, cost cannot be the determinant of the levels of rights protection afforded to individuals.

  We therefore recommend that the term "sensitive personal data" be clarified to also permit a context-specific application (just as in the case of the definition of 'personal data'). This would ensure that information that reasonably reveals sensitive personal data would also be included within the ambit of the phrase. In this context, please also refer to the comments made below pertaining to Section 22 of the Bill.

2.3 Data protection obligations: Fair and reasonable processing

Section 4 of the Bill lays down the duty to process personal data in a fair and reasonable manner that respects the privacy of the data principal. This is a particularly important principle given that the persons enjoying the exemptions given in Chapter IX of the Bill (security of state, prevention of offences, legal proceedings, research and statistical purposes, etc) are still bound by the requirements of this provision. The Bill adopts a principle-based approach in this regard, which is appropriate given that the provision will be applicable to a diverse range of persons and in a variety of circumstances. However, the broad nature of the provision can also lead to some concerns in terms of allowing too much discretion to the data fiduciary in deciding what constitutes "fair" and "reasonable". The broad nature of the term similarly vests a lot of discretion with the adjudication officers of the DPA in deciding whether the actions of the person satisfy such a threshold. It would therefore be useful for the principle to be supported by some guidance on factors to be considered while determining whether a particular conduct is fair and reasonable.

Article 5(1)(a) of GDPR provides that personal data must be processed *"lawfully, fairly and in a transparent manner"*. While the law does not define what is meant by the term "fair", it does find mention in other provisions. For instance, Article 13(2) provides a list of information that must be given to the data subject in order to "ensure fair and transparent processing". Further, Article 401(1) identifies this as one of the grounds on which codes of conduct may be framed. The Data Protection Act, 2018 that has been adopted by the United Kingdom, supplements some of the provisions of the GDPR. In the context of processing of data by intelligence service agencies, it provides that in determining whether the processing is fair and transparent, the method by which the data is obtained is relevant – for instance it would be fair if the data was obtained from a person authorised or required to supply it under law or an international obligation.[6]

Maxwell (2015) provides a detailed comparison of the fair processing principle as applied in the United States and Europe. In the U.S, Section 5 of the Federal Trade Commission (FTC) Act, 1914 prohibits "unfair or deceptive acts or practices in or affecting commerce". Following concerns that the FTC was using the unfairness standard in a very subjective manner, the U.S. Congress brought an amendment to ensure that FTC would refer to an objective methodology when evaluating questions of fairness. It required that in order to constitute unfairness the practice should be such that it causes *"substantial injury to consumers*

[6]Section 86(5) and (6), United Kingdom Data Protection Act, 2018.

which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."

Drawing from these discussions, we propose that the Bill should offer some guidance on the factors to be considered while determining whether a particular conduct can be regarded as fair and reasonable. Consequently, the DPA can frame codes of practice or regulations to provide the minimum requirements for fair and reasonable conduct in different contexts.

2.4 Grounds for processing of personal data and sensitive personal data

Sections 13 and 19 - Processing of personal data and sensitive personal data for the functions of the State

Sections 13(1) and 19(1) of the Bill allow processing of personal data without the consent of the data principal as long as such processing is "*necessary for any function of Parliament or State Legislature.*" Neither the Bill nor the Srikrishna Committee report give any indication as to the matters that may be covered under this sub-heading, especially considering that under section 2(3), they presumably cannot be achieved by using anonymised data.

Sections 13(2) and 19(2) go further in authorising non-consensual processing by the State if it is necessary, inter alia, "*for the exercise of any function of the State authorised by law for the provision of any service or benefit to the data principal.*" It is pertinent to note that the terms "service" or "benefit" have not been defined in the Bill. If the definitions and implementation of similar provisions in the Aadhaar Act are any indication, the exception under sections 13(2)(a) and 19(2) may become broader than the original requirement for consent, and undermine the steps taken towards strengthening consent (Bhandari & Sane, 2018). One way in which this ground for processing can be restricted is by introducing a requirement for "proportionality".

Although Sections 13 and 19 are still subject to Chapter II's mandate of fair and reasonable processing, collection and purpose limitation, there is no need for the measure to be proportionate. By introducing such a limitation on the power of the State to override consent, the rights of the data principal will be better safeguarded and they will be assured that the terms "any function" and "any service" will not mean "every" function and service. Such an amendment will also be consonant with the observations in the Srikrishna Committee Report, that "imbalance of power" in citizen-State interactions affects the validity of the consent given and

that the term "necessary" would mean that processing should be targeted and proportionate.

Finally, on the issue of sensitive personal data, we are of the opinion that the use of the phrase "strictly necessary", especially in contrast with phrases such as "necessary", "reasonably practicable" (section 8(1)), "not appropriate" (section 16(2)) and "reasonable purpose" (section 17(1)) leaves a lot of room for ambiguity. If section 19 is to serve as an actual constraint on State power, the Bill will have to give some directions on how these different phrases are to be construed, both in terms of standard of review and intensity of review.

Section 22 - Power of the Authority to notify additional categories of "sensitive personal data"

Section 22 permits the Authority to add categories of information to the definition of sensitive personal data (and indeed the Srikrishna Committee Report notes that certain types of data such as location data may be added to the existing list of sensitive personal data). The provision however, does not allow a relaxation of conditions or removal of categories of data from the list.

Given our previous comments on treating information as sensitive personal data based on context, we believe that the data protection authority must also have the power/ capacity to exclude certain types of data from the onerous conditions imposed for processing of sensitive personal data, if on facts, it is found that the processing in question is not particularly intrusive or likely to cause harm/significant harm. However, any such determination will have to be very carefully made so as to not reduce the privacy rights of the individual.

Concommitant changes will also need to be made to Section 60(c) of the Bill, which empowers the Authority to (only) specify residuary categories of sensitive personal data.

2.5 Personal and sensitive personal data of children

Section 23 deals with the processing of personal and sensitive personal data of children, where a child is defined in Section 3(9) to be a person below the age of 18 years. While this is in line with the age of majority in the Contract Act, the Srikrishna Committee report acknowledges that *"We are aware that from the perspective of the full, autonomous development of the child, the age of 18 may appear too high".* Given that there is some uncertainty around what should be the appropriate age to qualify as a child in this context, the law should at the very least include a principle that the determination of the "best interests of the child"

would vary depending on the age bracket that the child belongs to. This would allow data fiduciaries as well as the Authority the leeway to distinguish between the measures that would be regarded as being appropriate for a child of 5 years versus a child of 18 years.

The above suggestion also finds support from Article 5 of the United Nations Convention on the Rights of the Child, which requires States Parties to respect the responsibilities, rights and duties of parents and guardians, to provide, *in a manner consistent with the evolving capacities of the child*, appropriate direction and guidance in the exercise by the child of the rights recognised in the Convention.

Further, in recognition of the vulnerable status of children in society, we propose that the Bill should provide an explicit opt out mechanism, on attaining majority. Such a view is also consistent with the opinion of the majority in *KS Puttaswamy v. Union of India (2018)* (Aadhaar).

2.6 Transparency and accountability measures: Personal data breach

The provisions pertaining to data breach notification in **section 32** of the Bill are weak and require strengthening. First, the phrase "personal data breach" is not defined in the Bill. We suggest inclusion of a definition as the provision is critical in triggering notification and other requirements. There should be no confusion regarding what constitutes a data breach that requires action to be taken under Section 32. In this respect we note that the GDPR defines the phrase in Article 4(12) as *"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed"*. We suggest the adoption of a similar definition in the proposed Indian law.

Second, data fiduciaries should be required to report all instances of data breach. The reporting requirement should not be based on the data fiduciary recognising the possibility of harm to the data principal. Such a standard will lead to confusion and inadequate protections – it may be possible for a data fiduciary to deny reporting a data breach claiming that they assumed it would not cause harm. Equally, it is possible that the leaked information may itself not cause harm, but in conjunction with other data sets, that the fiduciary is unaware of, it could result in adverse consequences for an individual. This indicates that the determination of whether harm is caused should not be left entirely to the fiduciary. Such a position also mitigates against the purpose of privacy law, which is to ensure citizens have some measure of control over their data. The present provision effectively re-

duces the agency and autonomy of individuals, and their ability to make informed decisions about their personal data.

Third, it is unclear why the draft law adopts a two stage process for notification of data breaches and why only certain breaches are to be reported to the individual concerned. Such a system is likely to pose a significant regulatory burden on the Authority, requiring it to make subjective determinations on the possibility of harm to every individual affected, and leading to potential litigation. This system also mitigates against the autonomy of individuals – they are kept in the dark about what is being done with their personal data. A data principal, may for instance, wish to withdraw consent or otherwise object to processing should it appear that security measures adopted by the fiduciary are insufficient (i.e. the fact of a data breach may be a relevant factor in the risk-reward calculation done by a data principal while giving consent to processing). By not directly informing the data principal of a breach, the ability of a principal to make an informed decision about their data is lost.

Given the knowledge that an individual has about the data provided to a fiduciary and the context of providing such information, the person should have the opportunity to make a determination about the possibility of harm. For instance, the European Court of Human Rights has held in Klass v. Germany (1978) (although in a different context) that it is generally the individual concerned who is best placed to judge the severity and harm caused by intrusions into their lives.

While the European GDPR generally requires notification of data breaches to the individual concerned, this is not required where (a) security measures have been adopted to ensure that the breached data is unintelligible to unauthorised persons, (b) risks to privacy rights are unlikely to materialise due to ameliorative measures adopted by the controller, (c) it would involve a disproportionate effort on the part of the controller to inform each data subject – in which case public notification may suffice.

Accordingly, we propose that data fiduciaries must in general, be under an obligation to inform data principals of any data breach. However, in order to avoid placing disproportionate or onerous obligations on data fiduciaries, the Indian law could use similar measures as mentioned above, although condition (b) on ameliorative measures needs to be examined more critically as it interferes with user autonomy.

2.7 Transfer of personal data outside India

Sections 40 and 41 of the Bill propose a "three-pronged model" for international transfers of personal data. One live, serving copy of all personal data should be stored in India, in addition to which certain categories of "critical personal data" (a subset of sensitive personal data that would be notified by the government), will be bound by a stricter requirement of being stored and processed only in India. Finally, the government will have the power to exempt particular countries, sectors or international organisation from the restrictions on free flow of data across borders on the grounds of 'necessity' or 'strategic interests of the state'.

We disagree with the way the draft law attempts to deal with the issue of data transfers, and the absence of any cogent reasons or cost-benefit analysis conducted before taking this step.

First, the only grounds that the personal data protection law should concern itself with insofar as the adoption of localisation measures are concerned, is that of whether such measures would enhance privacy rights of individuals in India. While sovereignty, economic development and regulatory access are cited as reasons to require localisation – these are not reasons that directly enhance data protection. We recognise that the government may have numerous reasons to ensure localisation – from a strategic, social or economic perspective – however the present law deals with only privacy/data protection related rights, and as such, should only look to enable localisation where it is demonstrable that the privacy protections afforded by such a step are worth the trade-offs associated with localisation (in terms of restriction of expression and privacy rights, costs to businesses, etc).

An analysis of literature shows that location of data has no real bearing on its safety and security. While arguments may be made for and against the impacts of localisation on data privacy in any specific factual context, it is unclear whether mandatory localisation is always an appropriate or efficient means to achieving such an end (equally, permitting free trans-border flows of data will not in itself lead to enhanced privacy protections) (Bailey & Parsheera, 2018). Privacy and security of data ultimately depends on – (a) the technical measures, skills, cyber security protocols, etc., put in place rather than the mere location of data (Hill, 2014); and (b) appropriate legal/ technical frameworks to preserve privacy both locally and globally - for instance, through building in privacy by design mechanisms in networks and digital systems and encrypting user data (Sargsyan, 2016).

While localisation measures may in certain situations enhance privacy protections (assuming that the foreign location where the data is stored has a sub-optimum framework for data protection), they can also negatively impact rights (to expres-

sion and privacy) and lead to a huge cost to business, which is not justified by demonstrated gains. Given the ability to utilise numerous less intrusive measures to equally protect personal data of Indian citizens (such as binding contractual rules, need for adequacy decisions prior to transfer, etc.), we believe that the provisions requiring mandatory mirroring of personal data within India / complete localisation of critical personal data appear disproportionate and unnecessary and must be revisited.

This is not to say that localisation can never be a necessary or proportionate response to perceived harms from privacy – just that the specific harms must be identified, and then the costs and benefits of imposing such measures must be adequately demonstrated. We suggest therefore, that the personal data protection law itself contain no specific mandate pertaining to mirroring or complete localisation. To the extent that it may empower the DPA or the Government to direct the localisation of certain specific types of data / localisation by specific entities, it should specify a robust cost-benefit analysis and public consultation processes before arriving at such a decision (Bailey & Parsheera, 2018).

Finally, we note that Section 97(7) of the Bill empowers the Government to notify the provisions pertaining to cross border data flows at a time of its choosing. This implies that the said provisions may be brought into force at a different time to the rest of the statute, or indeed need not be brought into force at all. This will lead to further confusion amongst data fiduciaries and data principals alike, on account of the uncertainty that the the localisation notify. Further, it will also lead to competition distortions and uncertainty in the market for provision of cloud computing and data center services. As indicated above, the law should not announce any mandatory mirroring or complete localisation norms without a robust evaluation of the social and economic costs and benefits of such a move for different sectors. It may instead lay down the process for undertaking a detailed analysis of the harms expected to be caused by a particular international transfer of personal data and the costs and benefits of implementing such measures.

2.8 Exemptions

Sections 42 and 43 - Security of the State; Prevention, detection, investigation and prosecution of contraventions of the law

According to Sections 42 and 43 of the Bill, processing of personal data in the (i) interests of the security of the state; and (ii) for prevention, detection, investigation and prosecution of any offence or any other contravention of law is exempt from

most obligations[7] under the Bill, if it:

- is accordance with law,
- follows the procedure set out by that law (this requirement does not apply to Section 43), and
- is necessary and proportionate.

These provisions embed the proportionality standard set out by the majority in (Puttaswamy v. Union of India, 2017) (and confirmed more recently in KS Puttaswamy v. Union of India (2018)). The Bill, however, fails to address the related structural and procedural elements that are required to operationalise these principles. For instance, while the Bill lays down that the interception should be necessary and proportionate, it does not address the question of who should make this determination. The Srikrishna Committee's report acknowledges that the current processes under the IT Act and the Telegraph Act, which provide only executive review for such decisions, are not sufficient and recommends that district judges should be reviewing the processing of personal information by intelligence agencies in closed door proceedings. However, this requirement does not find mention in the text of the Bill itself. The importance of prior judicial review has also found support in the recent judgment of the Supreme Court in KS Puttaswamy v. Union of India (2018). Judicial authorisation for interception requests is also the norm in other liberal democracies such as the United States,[8] the United Kingdom,[9] and Canada.[10]

Apart from the issue of ex-ante judicial scrutiny of surveillance requests, the Srikrishna Committee's report also talks about ensuring accountability through ex-post, periodic reporting and review by a parliamentary committee. However, the Bill again does not provide for such ex-post reporting and review. The Committee's report suggests that these measures should be adopted if and when the Government decides to pursue a comprehensive law governing intelligence agencies.

[7]Specifically, entities falling under this provision are exempted from the obligations imposed under Chapters II (except Section 4 - pertaining to fair processing), III, IV, V, VI, VII (except Section 31 - pertaining to security safeguards), and VIII.

[8]The US requires intelligence and law enforcement agencies to obtain warrants, subpoenas and other court orders in order to conduct domestic surveillance activities. See Sections 2516-2518 of the Electronic Communication Privacy Act of 1986, 18 USC 2510-22.

[9]U.K's Investigatory Powers Act, 2016 the approval process by introducing a "double lock" mechanism under which the warrant issued by the Secretary of State is also subject to review by a Judicial Commissioner before it comes into effect

[10]Canada has a system of specially designated judges in the Federal Court to approve warrants requested by the Canadian Security Intelligence Service. Part II of the Canadian Security Intelligence Service Act, 1985 deals with "judicial control" on the procedures for application for warrant.

While the instant Bill is admittedly not the correct site for ensuring a complete overhaul of the intelligence apparatus, not least due to the organisation and structural changes that may be required within intelligence and law enforcement services, nonetheless, the Bill should have proposed these ex-ante and ex-post oversight mechanisms as amendments to the Telegraph and IT Acts and the procedural rules made under them (Bailey, Rahman, Bhandari & Parsheera, 2018).[11]

Further, while the Bill requires personal data processed by law enforcement agencies (LEAs) and intelligence authorities to be processed in a fair and reasonable manner and adopt security features such as encryption and de-identification of data, it does not include several other key requirements. To highlight a few examples, the agencies are fully exempted from the requirement to have data protection officers;[12] the obligation to provide (deferred) notice of surveillance to the concerned individual; and the right to challenge and seek appropriate redress against unauthorised surveillance activities (Bailey et al., 2018). It is therefore unclear why other user rights (access, rectification, retention, etc.) and data protection principles should not be made applicable even to such agencies – subject to situations where data protection obligations may actively interfere with the duties of these entities.

Rights of individuals must be restricted only to the extent that this is a proportionate response, which would include instances where such intervention is necessary in a larger interest. This would include instances where failure to impose such restrictions could have the effect of harming or interfering with the investigation / prosecution of offences. In this respect, one may note that the UK's Data Protection Act, 2018, contains a separate part (Part 3) detailing the application of six data protection principles to law enforcement agencies. LEAs are not, as a matter of course, excluded from all data protection obligations and individuals continue to have rights qua personal data held by LEAs. As laid down by the Supreme Court in Puttaswamy v. Union of India (2017) and KS Puttaswamy v. Union of India (2018), an interference with privacy rights must be necessary and proportionate in nature. Blanket exemptions would therefore not constitute adherence to the proportionality principle.

As noted by us in Bailey et al. (2018), we recommend that:

1. *Prior judicial review*: The current process of authorisation of surveillance requests by the executive needs to be amended to incorporate an element of

[11] This is particularly important given that the surveillance is already being carried out without adequate safeguards, and in the absence of any comprehensive law on the issue.

[12] Notably, Section 36 of the Bill requires private entities to appoint a data protection officer for carrying out various functions including providing guidance on fulfilling obligations under the statute, monitoring personal data processing activities of the data fiduciary etc.

prior judicial review. Post-facto judicial scrutiny should be provided for in cases of emergency. This review may be conducted through specialised courts designated for this purpose or by judicial members of an independent body, such as a Data Protection Authority. Any amendments to the current laws should lay down a procedure for appeal against the decision of the judicial body. The Bill should propose the adoption of the proposed structure by suggesting corresponding amendments to the Telegraph Act, IT Act and the rules framed under those laws.

2. *Procedural guarantees*: As stated earlier, Section 43 of the Bill grants exemptions from certain data protection obligations if the processing of personal data is in "the interests of prevention, detection, investigation and prosecution of any offence or any other contravention of law' and is first, authorised by a law made by Parliament and State Legislature, and second, is necessary for, and proportionate to, such interests being achieved. However, it is unclear why the provision drops the requirement for processing to be in accordance with the procedure set out under the authorising law (as stated under Section 42). The obligation to follow the procedure set out under the authorising law should be introduced in Section 43.

3. *Reporting and transparency*: Appropriate ex-ante and ex-post reporting and transparency obligations pertaining to all surveillance activities should be imposed on LEAs and intelligence agencies. Oversight bodies must also be required to publish periodic reports of their activities and that of LEAs/ intelligence agencies under their supervision, while service providers must be permitted to publish aggregated statistics detailing volume and nature of surveillance requests.

4. *Notice to data subject*: Further, the State should also have an obligation to provide deferred notice of interception to the concerned individual. However, the intelligence agency or LEA may seek the approval of the judicial body to delay or avoid the requirement of notice under certain exceptional circumstances, if, for instance, it can be established that such a disclosure would defeat the purpose of surveillance. Circumstances under which this exception can be invoked should be listed clearly.

5. *Right to seek redress*: The requirement of notice to the data subject must be accompanied by a right to challenge and seek appropriate redress against surveillance activities. This right should extend to a person who is, or has reasonable apprehension of being, the subject of surveillance. In addition, intermediaries that are under a legal obligation to facilitate access to information by LEAs should also have the legal right to question the scope

and purpose of the orders received by them.

6. *Privacy Officers*: Intelligence agencies and LEAs should have an obligation to appoint data protection officers. The data protection officer should be required to, inter alia, scrutinise interception requests by the agency (before they are put up to the sanctioning judicial body), ensure adherence to the relevant laws. Further, their considered opinion pertaining to interception requests must be recorded in writing and available to relevant oversight bodies (if not the public).

7. *General data protection rights*: With regard to personal data processed by LEAs and intelligence agencies, we recommend that the Bill must ensure that, as far as possible, data principals are provided with access and rectification rights, and personal data maintained by relevant authorities is up to date and accurate. Further, data retention norms also need to be appropriately designed to ensure only relevant data is stored by the authorised agencies. The exemptions provided under these sections must be narrowly tailored so as to ensure that necessary activities of law enforcement agencies do not suffer - however, the limitations must be strictly to such extent so as to avoid unnecessarily impinging on privacy rights of individuals.

Section 45 - Research, archiving or statistical purposes

Section 45 of the Bill permits the Authority to exclude the application of all parts of the law except Section 4, 31 and 33 to processing of personal data carried out for research, archiving or statistical purposes. We note a few concerns with the scope of this provision.

1. Artistic, literary and academic endeavours are currently not covered under the scope of the exemptions in the law despite all being areas where expression rights and the broader interests of society must be balanced with privacy rights. For instance, under the current provision, taking photographs or videos in public for artistic purposes, will require adherence to various obligations under the law including ensuring appropriate grounds of processing.[13] In certain situations, it may prove practically impossible to comply with some data protection obligations – for instance, if a photographer takes pictures of a festival (thereby showing a large crowd).

   The journalistic exemption will also not apply squarely if the work is entirely artistic in nature and not pertaining to current affairs etc. It may also become possible for individuals to harass authors if personal information is even

[13]The 'household use' exemption would not apply as the purpose of artistic work will be to display the works to the public / secure commercial gain.

unintentionally used in a work of literature (or intentionally used to make a larger point about the state of society, presence of corruption, etc.). The absence of any exemption for artistic/ literary work may therefore hamper artistic license and the freedom of speech and expression.

It may also be preferable to extend the protections to academic work (as opposed to only "research work"). The word 'research' indicates a systematic act or inquiry aimed at enhancing knowledge. 'Academic' is a slightly different term including within its ambit the pursuit of research, education and scholarship. Academic work can be of great social value and to the extent necessary, should be excluded from the scope of the data protection law. It is also to be kept in mind that a lot of academic work may in any event be subject to other institutional regulations and checks.

The GDPR has considered this issue in Recital 153 and Article 85, and requires member states to provide for appropriate derogations from the privacy law where necessary to protect journalistic, *academic, artistic or literary interests*. Thus, the UK for instance, excludes journalists, academic, literary and artistic material (in addition to research, statistics and archiving functions) from the scope of various obligations under the Data Protection Act, 2018.

2. The provision must be clarified to ensure that research / archiving etc. conducted for predominantly commercial purposes is not brought within the ambit of the provision. For instance, market research by consumer companies should not be exempted from the purview of relevant data protection requirements. Given that the draft law circumscribes the journalistic exemption by ensuring the content pertains to news, recent or current events, or is in public interest, possibly a similar standard could be applied to archival / research based work (i.e. a public interest requirement could be introduced to limit application of this exemption). Here it is to be noted that while Article 89 of the GDPR provides an exemption for research purposes, this is limited to "archiving purposes in public interest, scientific or historical research or statistical purposes." The UK applies a similar test - the publication/archive, etc. must be in public interest.

3. It is questionable why provisions pertaining to privacy by design, grievance redress, transparency, etc. are not made applicable to even such entities. The scope of exemptions should be limited in nature and proportionate to the possibility of harm being caused. Implementing procedural safeguards, while a cost, would not significantly affect the ability of such entities to carry out their primary functions. Such processes would however ensure

higher standards of protection of data across the board. We note that even the UK's Data Protection Act, 2018, only excludes the application of data privacy related obligations "*to the extent that the application of those provisions would prevent or seriously impair the achievement of those purposes*" - implying that only those obligations that significantly impact the ability of the specific organisations to carry out their business (such as archiving, producing literary works, etc.) should be excluded. There is no per se or general exemption from a vast swathe of privacy related obligations as in the draft Indian law.

Section 46 - Personal or domestic purpose

Section 46 exempts the processing of personal data (except the requirement of fair processing) by a natural person if used purely for personal or domestic purposes.[14] The exemption does not apply if there is a 'disclosure to the public' or the processing is undertaken in connection with 'any' professional or commercial activity.

The phrase 'disclosure to the public' is however not defined in the Bill. Further, what constitutes a publication may have different meanings under various laws. For instance, under the law pertaining to defamation, publication would include communication of the defamatory material to an person other than the person defamed. In the patents context, publication implies communication of information about an invention to any member of the public who is not bound by a duty to keep the information secret. Under copyright law, publication implies the communication to the public regardless of whether any member of the public actually views the work in question. By way of example, under copyright law, a work performed in private need not infringe the law (Wadehra, 2012).

In the privacy context, it is unclear for instance, whether the phrase would mean that the personal information should be accessible, as a matter of right, to any member of the public? For instance, would it include passing on personal information on a closed social media group? This absence of clarity will not only lead to sub-optimal protection and uncertainty over application of the law, it may also lead to the Authority being burdened with vague and unnecessary complaints. We therefore recommend that a specific definition of the phrase 'disclosure to the public' be introduced in the law. The phrase must be interpreted in a broad manner to include receipt of the relevant personal information by any third party (in the absence of a data fiduciary-data processor relationship or a legal contract).

Separately, it is unclear whether the application of Section 31 needs to be excluded

[14]Section 46 excludes application of Chapters II - except Section 4, Chapter III, IV, V, VI, VII and VIII to domestic/ household processing.

for cases of domestic or personal use. The safeguards applicable under Section 31 are in any case subject to a context specific determination (the provision requires security safeguards to be implemented taking into account the "nature, scope and purpose of processing"). Accordingly, we do not find a need to completely exclude the applicability of this provision under Section 46. Given that Section 46 does not contain any considerations as to the quantity/volume of information collected, or the nature of this information processed, it is possible that an individual may collect large quantities of sensitive personal data. Arguably, such data should be appropriately secured taking into account all relevant facts (including costs to the individual processing the data).

Section 47 - Exemption for journalistic use of personal data

Section 47 exempts journalistic organisations from application of all data protection obligations except that of fair processing and the need to ensure security safeguards.[15] The exemption is applicable only if the organisation in question can demonstrate that the processing complies with a code of ethics issued by the Press Council of India or any media self-regulatory organisation.

The requirement of subscription to a code of ethics issued by the press council or a 'media self regulatory organisation' is ill-conceived and may act to limit speech and expression rights. Today, numerous bloggers and other individuals use the online space to present news, opine on current events and expose matters of public interest that the mainstream media cannot or will not cover. Requiring all such individuals to adhere to an ethical code (which may practically come to mean a registration requirement) is not desirable from a normative perspective.

Equally, the meaning of the phrase 'any media self regulatory organisation' is also unclear. Will a self regulatory organisation established by any two news websites be considered sufficient to meet this requirement? Can an individual blogger prescribe a code of ethics for himself/herself so as to avail of the exemption under this section? To avoid the challenges emanating from this vagueness, we recommend that the concept of 'public interest' can be used instead to justify the application of the journalistic exemption. The job of the Authority should not be to determine if someone is a journalist or not – but rather whether a particular piece of personal information is relevant to the public or required to be kept confidential in view of the consequences it may have on privacy rights of individuals. While Section 3(25) defines 'journalism' in a manner that includes the aspect of 'public interest', we do not believe that the privacy authority should be empowered to scrutinise media

[15]Section 47 exempts the application of Chapter II except Section 4, Chapters III, IV, V, VI, VII (except Section 31) and Chapter VIII of the draft law as far as journalistic uses of personal data are concerned.

ethics codes, editorial standards or other such aspects in any enquiry conducted under Section 47.

In this regard, we note that the UK's Data Protection Act, 2018, also requires the data controller to take into account public interest in deciding whether to publish personal data. Per Schedule 2, Part 5 of the said Act, *"in determining whether it is reasonable to believe that publication would be in the public interest, the controller must have regard to any of the codes of practice or guidelines listed in sub-paragraph (6) that is relevant to the publication in question"*. Thus, it is clear that signing up to a media code is not mandatory or a condition precedent to claiming the exemption under the provision. The reference to the media codes is only to the extent that these may prove useful in establishing objective conditions to show the 'public interest' nature of any reportage.

It is also unclear why the provisions pertaining to privacy by design, transparency, carrying out of impact assessments, record keeping, data audits, appointment of a data protection officer, classification as significant data fiduciaries and grievance redress are not made applicable to data fiduciaries who may claim the journalist exemption. The provisions in Chapter VII of the law are general procedural principles that will not necessarily impede the ability to carry out research or reportage. For instance, putting in place a grievance mechanism will not affect use of personal information for journalistic purposes. It would however permit individual's who believe their rights are being affected to make a complaint to the entity concerned. Similarly, putting in place privacy by design measures is generally good practice and should be encouraged across sectors.

It also makes little sense to permit journalistic organisations for instance, to use technology standards that are not up-to-date (Section 29(c)) - this will merely invite instances of hacking and breach. We note in this regard that the UK Data Protection Act, 2018, specifically exempts obligations only "to the extent that the controller reasonably believes that the application of those provisions would be incompatible with the special purpose".[16] The onus to show such conditions existed would be on the entity seeking exemption from the obligations under the privacy law.

Exemptions should be carved out only to the extent required for the entity concerned to go about their business (whether it is prosecuting offences, carrying out surveillance by the state, journalistic activities, etc), without interfering in individual's rights or exposing them to harm in a disproportionate or unnecessary manner. While making these provisions applicable to journalists may constitute a cost, it will also ensure that certain minimum standards of data protection are

[16]Refer Schedule 2, Part 5 of the UK Data Protection Act, 2018.

maintained across the digital ecosystem. Further, as recognised in the Srikrishna Committee's report, cost on its own cannot be a reason to avoid imposition of data protection obligations.

Section 48 - Manual processing by small entities

This section permits entities to avoid application of various provisions of the data protection law[17] subject to certain minimum thresholds being met (turnover of INR 20 lakhs in the previous financial year, do not disclose data to other entities, and have not processed data of more than 100 people on one day in the previous year). The rationale behind these thresholds is unclear. The threshold amounts (INR 20 lakhs, 100 individual's data being processed on one day) appear fairly low and could impose high costs on small enterprises. Local shops and services etc., and other small enterprises are likely to be unable to take advantage of the exemption due to the low thresholds.

Accordingly, the threshold amounts should be revisited to either calibrate them more appropriately, or preferably, to ensure context specific determination can take place of the likelihood of harm / risk involved in the processing in order to avail of the exemption.

Overall, we believe the law should reflect principles of risk based regulation. The obligations on an entity must be proportionate to the possibilities of harm caused by a specific type of processing (say in view of the nature of processing, the volumes of data processed, etc.). Generally speaking, all but the very smallest entities must be brought within the fold of the law, though the obligations on smaller entities must be lower than that on bigger entities. We note that Section 31 of the draft law includes such a risk-based test in the application of security measures. We recommend that such a risk-based regulatory method must be followed throughout the law.

2.9 Data Protection Authority of India

Composition of DPA

Section 50 of the Bill provides that the DPA will consist of a Chairperson and six whole-time members. It however, does not provide for any part-time or non-executive members. Such non-executive members can serve the important function of serving as neutral observers in the functioning of the DPA and alert the Government of any non-compliance of law by it. Further, they can also strengthen the

[17]The section excludes small entities from application of Sections 8, 9, 10, 24(1)(c), 26, 27, 29-36, 38, and 39 of the draft law.

working of the DPA by bringing in data protection expertise from the industry, academia and other avenues (FSLRC, 2013). The Srikrishna Committee's report does not offer any explanation as to why this element, which is also seen in laws governing agencies like the Securities and Exchange Board of India (SEBI) and the Telecom Regulatory Authority of India (TRAI), was not considered relevant in case of the DPA (Parsheera, 2018). We recommend that the Government should reassess the composition of the DPA by weighing the advantages of having a set of part-time or non-executive members in the DPA.

Processes of Selection Committee

Section 50(3) of the Bill provides that the Government will make rules to prescribe the procedures of the selection committee constituted for recommending names of DPA members. As submitted in our response to the White Paper, the integrity of the selection procedure needs to be protected by requiring that all short-listing and decision making by the committee is done in a transparent manner (Bhandari et al., 2018). For this purpose, the primary law should incorporate a certain level of detail regarding the processes of the selection committee. For instance, it should require the committee to disclose all the relevant documents considered by it and prepare a report after the completion of the selection procedure. This would include the minutes of the discussion for nominating names, the criteria and process of selection and the reasons why specific persons were selected (Parsheera, 2018).

Meetings of the Authority

Section 54 provides that the Government will make rules to prescribe the procedures to be followed for meetings of the DPA. As noted above in the case of the selection committee, it is important for the data protection law to also provide further details regarding the transparency and processes expected to be followed by the DPA in its own meetings. For instance, it should require that the agenda papers and the decisions taken in the DPA's meetings to be published and details of how each member voted on a particular matter to be made available publicly.

Annual report of the DPA

Section 48 of the Bill requires the DPA to prepare an annual report giving a summary of its activities during the previous year, leaving it up to the Government to prescribe the form and time of the report. For the annual report to really serve as a tool of accountability, the law needs to offer a more granular description of what is it that should be in the annual report. It should, for instance, include

items like details of the deliberations held in the Authority's meetings; reasons for non-compliance with any statutory functions; and list of major activities proposed for the subsequent year (Parsheera, 2018).

Coordination with other agencies

Section 67 of the Bill provides for coordination between the DPA and other agencies. This is a welcome provision but we point to the need for certain clarifications in its scope.

1. The Bill restricts the coordination requirement only to other statutory agencies but there may be situations where certain regulatory actions fall directly within the domain of a Ministry or Department of the Government. For instance, it may be relevant for the DPA to co-ordinate directly with the Ministry of Company Affairs or with the Health Ministry under certain circumstances.

2. It is not clear as to how it will be determined whether the other body has "concurrent jurisdiction" with the DPA. Instead of leaving this determination entirely up to the DPA it would be advisable for the Bill itself to contain a a non-exhaustive list of such matters and agencies with corresponding amendments to those laws requiring them to undertake similar co-ordination with the DPA. In addition, the Government may prescribe other matters and agencies to be covered in the list.

3. The term "any action" by the Authority needs to be clarified while considering whether such coordination is also expected to be done in case of adjudication of individual complaints by adjudication officers. We have separately commented on the limitations of this structure of giving adjudication powers to the DPA.

4. The Bill makes it discretionary for the DPA to enter into memorandums of understanding (MOUs) with other agencies. We recommend that this requirement should be made mandatory and the Bill should also set out a non-exhaustive list of the matters to be covered in the MoU. For instance, the MoU between the Financial Conduct Authority and the Information Commissioner's Office in the United Kingdom provides for sharing of information between the agencies and relevant confidentiality clauses, co-operation in framing rules and codes of conduct, complementarity in awareness activities, exchange of views in enforcement and investigation actions and referral of matters to one another (ICO and FCA, 2014).

DPA's regulation-making process

The Bill empowers the DPA to issue three main types of instruments: regulations (Section 108) codes of practice (Section 61), directions (Section 62). It is a well recognised principle of regulatory governance that any decisions that impose costs on those who have to comply with regulation or have an impact on how the market functions, should be based on factual information about the problem to be addressed, the cost incurred by a regulation, the effect of the intervention and the benefits expected to be achieved from it (Dudley & Wegrich, 2016).[18] While Section 61(4) takes a welcome step in requiring the DPA to issue "codes of practice" only after following a consultative process, a similar requirement has not been provided for the issuance of regulations and directions by the DPA.

In general, the law should incorporate a broader requirement of transparency in the discharge of all the functions of the DPA followed by provisions to specify what it would be require to act transparently in certain situations, for instance while framing regulations. As noted by us in Bhandari et al. (2018), effective public participation in the regulation-making processes of the DPA will ensure a system of checks and balances while also helping to improving its information and analysis systems. Further, the DPA should also be mandated to undertake an assessment of the expected costs and benefits of the proposed regulation and seek to adopt measures that minimise the compliance costs while meeting the intended objectives of regulation. Finally, the law should also mandate the DPA to provide an explanation for the decision finally adopted by it and the broad reasons for acceptance or rejection of the comments received from various stakeholders.

Powers of adjudication

The structure of the DPA, as envisaged by the Bill, involves a separate adjudication wing comprising of adjudicating officers, with the authority to impose penalties under Sections 69-73 and award compensation to individuals under Section 75. Under Section 68(2), the Central Government has complete power to prescribe the number of officers, their qualifications, their terms of appointment, jurisdiction, and procedures for carrying out adjudication under the Act, and any other requirements that the government deems fit. We point to the following concerns with the structure.

1. Section 68 raises a structural issue in terms of housing both the regulatory and adjudicatory functions within the DPA, a fact that was raised by us in our White Paper and also criticised by Justice Chandrachud in his dissent in the Aadhaar judgment (in the context of the UIDAI). Entrusting the DPA

[18] Also see FSLRC (2013).

with the responsibility of adjudicating individual complaints in addition to its regulation-making, supervision and enforcement functions can lead to the dilution of the core functions of the DPA and result in a conflict on interest.

As noted by us in Bhandari et al. (2018), a segregation of the regulatory and redress functions is particularly important in the context of the DPA given the principles-based nature of the proposed law. In such a scenario, the primary duty of the DPA should be that of formulating appropriate regulations on different provisions and for different contexts and conducting supervision activities to ensure compliance with the law. The large number of data fiduciaries in the system and the data principles who interact with them, coupled with the principles-based nature of the law implies that a large number of complaints are likely to come up before the DPA. In such a scenario, expecting the same set of adjudication officers to undertake enforcement functions as well as adjudication of individual cases would invariably cause one of these functions to suffer, both at the level of the adjudication wing as well as the DPA as a whole.

Another important reason to separate the functions of regulation and redress stems from need to avoid any conflict of interest that may arise from making the same agency responsible for the framing of regulations and providing redress for their breach. A large number of complaints on a particular issue not only reflects that data fiduciaries have not been acting in compliance with their requirements but also that the DPA may have failed to take appropriate regulatory or supervisory actions to curb such malpractices. It is therefore important that the resolution of any complaints should take place independent of the other core functions of the regulator (Bhandari et al., 2018).

Accordingly, we recommend that the redress of individual data protection complaints should be entrusted to a separate redress agency or ombudsman, that will function independently on the DPA. There should however be a strong feedback loop between the proposed ombudsman and the DPA using which the DPA can gain information about the type of complaints being raised, the entities to which they relate and the underlying causes. This will enable the DPA to address such issues through appropriate amendments to it's regulations or by initiating enforcement actions against particular data fiduciaries. Further guidance on issues relating to the proposed design, functions, human resource and other requirements of the proposed ombudsman can be drawn from the report of the Task Force on the Financial Redress Agency that was set up by the Ministry of Finance to discuss a similar mechanism in the financial sector.

2. In case the government decides to proceed with the Bill's recommendations on housing the complaints redress function within the DPA, there is still a case for bringing certain improvements in the proposed design and structure of the process. The current provisions of the Bill provide that any complaint raised by a data principle would directly proceed to determination by an adjudication officer (after the individual has first approached the data fiduciary's internal redress mechanism). We note that instead of directly sending the compliant for adjudication, there is a case for first attempting to facilitate an amicable settlement between the individual and the data fiduciary through a mediation process. In cases where the parties fail to reach a settlement the matter could then proceed for adjudication. Creating such a mechanism in the law would reduce the burden being cast on adjudication officers and expedite the settlement of grievances.

Committees to advise the DPA

We reiterate the proposal made by us in Bhandari et al. (2018) that that the law should empower the DPA to appoint various committees as may be necessary to assist it in the discharge of its functions. It would also be useful for the law to put in place a multi-stakeholder committee that can advise the DPA on the framing of standards that may be applicable in different contexts and the interpretation of the data protection principles laid down in the law. The "Article 29 Working Party" in the European Union could be a useful example for incorporating such a mechanism in the Indian data protection law. This Data Protection Working Party was established by Article 29 of Directive 95/46/EC, consisting of representatives of national supervisory authorities, European Data Protection Supervisors and a representative of the European Commission. The role of the Working Group is to provide the European Commission with independent advice on data protection matters and helps in the development of harmonised policies for data protection in the EU Member States.

2.10 Penalties and remedies

Sections 69 of the Bill provides that upon contravention of certain provisions of the Bill, the data fiduciary shall be liable to a penalty which may extend upto 2 percent or 4 percent of its total worldwide turnover in the previous year, depending on the nature of the offence. The term"total worldwide turnover" is defined in the explanation to the provision. We would like to highlight the following two points in this context.

First, since the scope of the Bill covers both State agencies and the private sector, it is important to note that the actual implementation of this provision against the State can be challenging as the "turnover" for the State is undefined. Further, monetary penalties against the State may not have the same disincentive, as against private parties, since the burden is eventually borne by the tax payers. This implies that regulating the actions of the State to generate desirable data protection outcomes may require more focus on mechanisms like departmental inquiries and internal actions, aside from the supervision by the DPA (Bhandari & Sane, 2018).

Second, we agree that the penalty on "worldwide turnover" can serve as an effective check in case of global businesses, particularly those that do not have a significant domestic presence and therefore may not have the incentive to invest in effective data protection mechanisms. However, it would also be relevant to point here to the experience of the Competition Commission of India while imposing penalties under a similar provision. While looking into the meaning of the term "turnover" in Section 27(b) of the Competition Act, 2002, which prescribed a penalty of *"not more than 10 per cent of the average of the turnover for the last three preceding financial years"*, the Supreme Court held that in the absence of a specific definition of the term, "turnover" in the legislation, it would be appropriate to limit the penalty too only the "relevant turnover". The Court found this to be in tune with the ethos of the Act and legal principles such as proportionality and equitable outcomes that govern determination of penalties. Further, it was held that for a company engaged in different areas of production, the "relevant turnover" would mean the turnover from the sales of goods or services, which are found to be the subject of contravention.

The outcome of CCI's case can easily be distinguished from the provision in the Bill, which specifically refers to the entity's worldwide turnover and goes on to define the term. However, the possibility that courts may subsequently try to limit the DPA's penalty powers to the relevant portion of the global turnover cannot be discarded, especially in case of global conglomerates that operate multiples lines of businesses.

2.11 Offences

Sections 90 and 91 of the Bill create criminal offences by penalising a person who "knowingly or intentionally or recklessly" commits the following acts in contravention to the Bill:

- obtaining, transferring, disclosing and selling of personal data such that it

results in significant harm to the data principal (Section 90);

- obtaining, transferring, disclosing and selling of sensitive personal data such that it results in harm to the data principal (Section 91); and
- re-identification and processing of previously de-identified personal data without the consent of data fiduciary or data processor (Section 92).

In addition, the Bill prescribes stringent punishment of imprisonment[19] and makes the above mentioned offences cognizable and non-bailable. The criminalisation of these actions and their categorisation as non-bailable and cognizable offences poses some concerns.

The White Paper stated that criminal sanction in the form of imprisonment and fines may be prescribed to ensure that it adversely affects the data controller financially and reputationally thereby serving some deterrent value. However, there is empirical research to demonstrate that the threat of imprisonment has only a small general positive deterrent effect (Ritchie, 2011).[20] The use of criminal sanctions in data protection laws is also seen in some other cases but the context and scope of those provision is different.

For instance, U.K's Data Protection Act makes it an offence for a person to knowingly or recklessly, *without the consent of the data controller*, obtain or disclose personal data or deal with it in any other manner. It is pertinent to note here that that unlike the provisions of this Bill, which apply to any person, including the data fiduciary, the UK law is much narrower in that it covers those persons who use personal data without *"the consent of the data controller"*. This would, for instance include a hacker who breaches the security safeguards of the data controller to gain unauthorised access to their data. Further, the UK law restricts itself to prescribing fines as penalty and does not lay down imprisonment as punishment for contravention.[21] The same is also true for Canada's PIPEDA wherein a capped fine is prescribed as penalty for offences that have been created under that law.[22] In case of the GDPR, Article 84 allows member states to lay down rules on other penalties applicable to infringements of the regulations, especially those infringements, which are not subject to administrative fines.

[19]For a term not exceeding three years for Sections 90 and 92 and a term not exceeding 5 years for Section 91.

[20]General deterrence seeks to reduce crime by directing the threat of criminal sanction at all probable criminal offenders. Specific deterrence, on the other hand, seeks to reduce crime by applying a criminal penalty to a specific offender, in order to dissuade him from reoffending (Ritchie, 2011).

[21]Section 196 of the U.K Data Protection Act, 2018.

[22]See Section 28, PIPEDA.

Further, stringent punishments such as imprisonment should not be imposed based on vague definitions and differing standards of "harm" and "significant harm". It is a well settled legal principle that criminal provisions must be precise and not overbroad (Sherya Singhal v. Union of India, 2013).

Finally, we note that the provision as currently drafted also criminalises ethical hacking or other forms of security related research, including into the effectiveness of anonymisation techniques. Today, numerous security failures are actually exposed by researchers and technologists working in public interest. It is often not in the interests of the data processing entity to give permission to allow its systems to be security tested thoroughly - due to the reputational and other harms that may occur. Equally, the current provisions of law may stop researchers from identifying problems with anonymisation methods – as re-dentification of data is an offence.[23]

In this context, we note that UK's Data Protection Act specifically lists various defences that could be taken against the offence of unlawfully obtaining or dealing with personal data (Section 170), and against re-identification of personal data (Section 171) - notably on the ground of public interest.

Section 172 of UK's Data Protection Act lays out the conditions for claiming the aforesaid exemption/defence under Section 171. Notably, the defence in Section 171 may be adopted if the person acted (a) with a view to testing the effectiveness of the de-identification of personal data, (b) without intention of causing harm or distress, etc., (c) in the reasonable belief that there was a public interest behind the re-identification of information. The person must also notify the relevant authorities or the controller responsible for the anonymisation about the re-identification of the data, without undue delay, and where possible within 72 hours of becoming aware of the de-identification.

We submit that Sections 90, 91, 92, and 93 of the Bill should be revisited in light of the above discussions.

[23] See Pauli (2016) and (Olejnik, 2017).

References

Anderson, N. (2009). ‘‘anonymized” data really isn’t and here’s why not. ArsTechnica , September. Retrieved from https://arstechnica.com/tech-policy/2009/09/your-secrets-live-online-in-databases-of-ruin/

Article 29 Working Party. (2007). Opinion 4/2007 on the concept of personal data. European Commission, WP 136, 01248/07/En, June 2007. Retrieved from http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf

Al-Azizy, D., Millard, D., Symeonidis, I., O’Hara, K. & Shadbolt, N. (2015). A literature survey and classifications on data deanonymisation. Springer International Publishing. Retrieved from https://www.esat.kuleuven.be/cosic/publications/article-2576.pdf

Bailey, R. & Parsheera, S. (2018). Data localisation in india: questioning the means and ends. NIPFP Macro/Finance Group (forthcoming).

Bailey, R., Rahman, F., Bhandari, V. & Parsheera, S. (2018). Use of personal data by intelligence and law enforcement agencies. National Institute of Public Finance and Policy, MacroFinance webpage. Retrieved from http://macrofinance.nipfp.org.in/PDF/BBPR2018-Use-of-personal-data.pdf

Bhandari, V., Rahman, F., Parsheera, S., Kak, A. & Sane, R. (2018). Response to the white paper on a data protection framework for india. National Institute of Public Finance and Policy, MacroFinance webpage, 31 January 2018. Retrieved from http://macrofinance.nipfp.org.in/PDF/BKPRS2018WhitePaperResponse.pdf

Bhandari, V. & Sane, R. (2018). Protecting citizens from the state post puttaswamy: analysing the privacy implications of the justice srikrishna committee report and the data protection bill, 2018. Socio-Legal Review, forthcoming.

Crowther, B. T. (2012). (un)reasonable expectation of digital privacy. BYU Law Review, Volume 2012, Issue 1, Article 7. Retrieved from https://bit.ly/2OoDfqT

Dudley, S. E. & Wegrich, K. (2016). The role of transparency in regulatory governance: comparing us and eu regulatory systems. Journal of Risk Research, Vol 19, 2016, p. 1141-1157.

FSLRC. (2013). Report of the financial sector legislative reforms commission. Volume 1: Analysis and Recommendations, March 2013. Retrieved from https://dea.gov.in/sites/default/files/fslrc_report_vol1_1.pdf

Galic, M., Timan, T. & Koops, B.-J. (2016). Bentham, deleuze and beyond: an overview of surveillance theories from the panopticon to participation. Tilburg

Law School Legal Studies Research Paper Series No. 13/2016. Retrieved from http://ssrn.com/abstract=2817813

Gambs, S., Killijian, M.-O. & del Prado Cortez, M. N. (2014). De-anonymization attack on geolocated data. Journal of Computer and System Sciences, Elsevier, 80 (8). Retrieved from https://hal.archives-ouvertes.fr/hal-01242268/document

Hares, D. R. (2015). Selection and implementation of expanded codis core loci in the united states. Forensics Science International: Genetics, Volume 17, July. Retrieved from https://bit.ly/2DHmi6E

Hill, J. (2014). The growth of data localization post-snowden: analysis and recommendations for u.s. policymakers and industry leaders. The Lawfare Institute, Lawfare Research Paper Series, Vol.2, No.3, July. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2430275

ICO and FCA. (2014). Memorandum of understanding between the financial conduct authority and the information commissioner's office. Government of UK, 29 September, 2014. Retrieved from https://ico.org.uk/media/about-the-ico/documents/1560123/mou-financial-conduct-authority.pdf

Kerr, O. S. (2007). Four models of fourth amendment protection. Stanford Law Review, Vol 60. Retrieved from https://bit.ly/2zLm4Y

Kistner, B. M. (2016). The fourth amendment in the digital world: do you have an expectation of privacy on the internet? Law School Student Scholarship, Paper 830. Retrieved from https://bit.ly/2O17ODL

Klass v. Germany. (1978). European Court of Human Rights, A 28 (1978), 2 EHRR 214.

KS Puttaswamy v. Union of India. (2018). WP (Civil) No. 494 of 2012, available at https://www.sci.gov.in/supremecourt/2012/35071/$35071_2012_{Judgement_26-Sep-2018.pdf}$..

Law Commission of India. (2017). Human dna profiling - a draft bill for the use and regulation of dna based technology. Government of India, Law Commission Report No. 271. Retrieved from https://bit.ly/2zIJVI6

Maxwell, W. J. (2015). Principles-based regulation of personal data: the case of "fair processing".

Narayanan, A. & Shmatikov, V. (2008). Robust de-anonymization of large sparse datasets. 2008 IEEE Symposium on Security and Privacy, Washington DC. Retrieved from https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf

National Research Council Committee on DNA Technology in Forensic Science. (1992). Dna technology in forensic science. Chapter 5: Forensic DNA Databanks and Privacy of Information, National Academies Press, Washington, USA. Retrieved from https://www.ncbi.nlm.nih.gov/books/NBK234540/

Nissenbaum, H. (2004). Privacy as contextual integrity. Washington Law Review, February. Retrieved from https://crypto.stanford.edu/portia/papers/RevnissenbaumDTP31.pdf

Olejnik, L. (2017). Reidentification ban is not a solution. Security, Privacy and Tech Inquiries Blog, 7 August, 2017. Retrieved from https://blog.lukaszolejnik.com/reidentification-ban-is-not-a-solution/

Parsheera, S. (2018). Data protection bill: lukewarm effort towards strong dpa. The Quint, 4 September. Retrieved from https://www.thequint.com/voices/opinion/data-protection-draft-bill-foundation-of-dpa

Pauli, D. (2016). Researchers crack oz govt medical data in easy attack with pcs. The Register, 29 September, 2016. Retrieved from https://bit.ly/2pJMh3w

Puttaswamy v. Union of India. (2017). 2017 (10) SCC 1, Supreme Court of India.

Ritchie, D. (2011). Sentencing matters: does imprisonment deter? a review of the evidence. Sentencing Advisory Council, State Government of Victoria, April 2011. Retrieved from https://tinyurl.com/y7awcdb

Rushe, D. (2014). Facebook sorry 'almost' for secret psychological experiment on users. The Guardian, October, 2014. Retrieved from https://www.theguardian.com/technology/2014/oct/02/facebook-sorry-secret-psychological-experiment-users

Sargsyan, T. (2016). Data localisation and the role of infrastructure for surveillance, privacy and security. International Journal of Communication, Vol. 10, 2221-2237. Retrieved from ijoc.org/index.php/ijoc/article/viewFile/3854/1648

Schneier, B. (2009). Its time to drop the 'expectation of privacy' test. Wired, March 26, 2009. Retrieved from https://www.wired.com/2009/03/its-time-to-drop-the-expectation-of-privacy-test/

Sherya Singhal v. Union of India. (2013). (2013) 12 SCC 73.

Simmons, K. C. (2015). Future of the fourth amendment: the problem with privacy, poverty, policing. University of Maryland Law Journal of Race, Religion, Gender and Class, Volume 14, Issue 2, Article 3. Retrieved from https://core.ac.uk/download/pdf/56360400.pdf

Solove, D. (2006). A taxonomy of privacy. University of Pennsylvania Law Review, Vol 154, No. 3, January. Retrieved from https://bit.ly/2Nj0ePD

Wadehra, B. (2012). Law relating to intellectual property. New Delhi, India: Universal Law Publishing Co.

Zhukova, A. (2017). Facebook's fascination (and disturbing) history of secret experiments. MakeUseOf, April, 2017. Retrieved from https://www.makeuseof.com/tag/facebook-secret-experiments/