COMMENTS ON THE PERSONAL DATA PROTECTION BILL, 2019

Submitted by Tandem Research, 25 February 2020

The Personal Data Protection Bill, 2019 (hereinafter referred to as “the Bill”) is the result of India's tumultuous journey in safeguarding the right to privacy and data protection of the citizens of India. As the Bill, which was introduced in the Lok Sabha in December 2019, moves further toward becoming legislation, the Joint Parliamentary Committee, headed by Chairperson Meenakshi Lekhi, has invited comments and suggestions on the Bill from public and private stakeholders.

Tandem Research is an interdisciplinary research collective that generates policy insights at the interface of technology, society, and sustainability. We believe that evidence-based policy, supported by broad-based public engagement, must steer technology and sustainability trajectories in India. Our work seeks to ensure that no one gets left behind in the technology transitions shaping India’s future. We appreciate the opportunity to submit our suggestions toward ensuring a well-founded data protection framework is established in India, and would also like to express our willingness to appear before the Committee to this end.

Below is a summary of our key concerns, followed by a detailed chapter wise comments and suggestions.

KEY CONCERNS

The proposed Legislation seeks to bring a strong and robust data protection framework for India and to set up an Authority for protecting personal data and empowering the citizens with rights relating to their personal data, ensuring their fundamental right to "privacy and protection of personal data".

We do not believe the Bill provides adequate privacy protections to citizens, particularly with regard to the processing of personal data by government authorities. Further, while we believe there is tremendous benefit to establishing the fiduciary relationship proposed by the Bill, the Bill falls short in adequately defining fiduciary responsibilities and identifying a basis of trust, placing instead an unreasonable and unrealisable responsibility on citizens to safeguard their own privacy. Rather than providing adequate protections, the Bill better identifies the conditions under which considerations of privacy can be side-stepped by both private enterprises and government agencies. The current approach risks subsuming privacy concerns to priorities of economic growth and national security, while increasing the surveillance capacities of the state. With revisions, the bill could provide an important baseline or starting point for data protection and privacy. However, other types of intervention that promote and enable responsible data stewardship - strengthening the trustworthiness of those who use and hold data - will need to be seriously examined if users are to gain better control over their data. Equally, we will need to develop frameworks and conditions for the legitimate collection and use of data, with clearly specified and transparent accountability provisions. Current provisions, such as those around the composition of the Data Protection authority and exemptions for government agencies, undermine rather than contribute to such trust building. Further, the Bill includes a number of vague and under-specified terms, such as public benefit and innovation, which are used to grant critical exceptions to the Bill; nor does the Bill specify a timeline for implementation.

1. DATA AND ITS STEWARDSHIP

The Bill views data as a national asset, an economic resource, that should be leveraged for growth and development. This framing is also found in other recent government documents - the recent Economic Survey[1] and Draft National Strategy for AI[2] are pertinent examples. We find this framing problematic. While data driven technologies can certainly make significant contributions to societal wellbeing and economic growth, harnessing this potential must not be at the expense of individual rights and social and justice. The provision in the Bill that allows the Government to access non-personal data by directing data fiduciaries is thus deeply problematic, as it subsumes individual rights and protections to broader objectives of economic growth and development, particularly as new techniques allow personal data to be identified back to individuals.

1 Economic Survey of India, 2018-2019 <https://www.indiabudget.gov.in/economicsurvey/> accessed 23 February 2020

2 NITI Ayog, 'National Strategy on Artificial Intelligence' (NITI Ayog, 4 June 2018) <https://niti.gov.in/sites/default/files/2019-01/NationalStrategy-for-AI-Discussion-Paper.pdf> accessed 23 February 2020.

We need to explore alternative frameworks for data stewardship that balance these competing values in a meaningful way, rather than uncritically subsuming one under the other, as is currently the case in the Bill. An important step in balancing these objectives is to shed framings of data as an economic resource, that is to be extracted and maximized. Rather, we must recognise data as embodied i.e. as being an extension of our bodies[3]; as situated i.e. as embedded in, and reflective of, societal values and priorities; and as networked i.e. emerging through interaction between and across human and physical environments. This framing of data also implies that the distinctions in the bill around personal data, sensitive data, and non-personal data do not hold - whether data is sensitive or not will depend on the context in which it is collected and used, and even seemingly non-personal data is likely to significantly impact individuals.

2. INADEQUACY OF A CONSENT BASED MODEL

The Bill defines the obligations of data fiduciaries in terms of consent and purpose limitation. This is likely to be inadequate for a number of reasons. It assumes that choices are free and informed, but this is not always the case. Withholding consent can often result in denial to essential services, and exclusion from socio-economic life. Privacy notices are typically buried in heavy legal jargon, and are framed to protect organisations, rather than users. People also have consent fatigue, and differing capacities to making meaningful choices around consent. Furthermore, with new machine learning and AI, it is impossible for individuals to know how and when their data is being used. AI technologies also rely on a large amount of data - the more data, the better - their workings are thus in contrast to the aim of purpose limitation and data minimisation. AI also works better with longitudinal data, increasing thereby the utility of storing data for future use. In the case of health for example, AI needs as much patient data as possible, in much detail as possible, to be able to identify and establish correlations. This patient data could then be used to provide health care services, but also develop enable the company to develop new products, unknown to the patient. Moreover, in automated data collection or 'smart environments', there is little opportunity for any real notice and consent, nor purpose limitation. In its current framing, because of the clear limitations of a framework based on consent and purpose limitation, the Bill provides a legitimate way for data fiduciaries to circumvent their responsibilities while still complying with the law.

The excessive powers afforded to the Government through exemption from consent adds to the inadequacy of the framework. It is important that the Bill stay true to the trust based relationship it aims to establish. For this, we need to look beyond consent based frameworks and instead develop conditions and limits around legitimate data collection and use. This should be done through deliberative and participatory processes that explore public understanding of fair exchange of data across various domains, and develop institutions of trust and credibility that are capable of responsible data stewardship. The Bill introduces the ideas of a consent manager and data trust scores, but these are not elaborated upon, and would merit further exploration.

3 Anja Kovacks, Data Governance Network / Internet Democracy Project.

3. UNDERESTIMATION OF ALGORITHMIC DECISION MAKING SYSTEMS

Despite the growing use of algorithmic decision making systems and artificial intelligence by government agencies and private actors, these are not adequately considered in the Bill. Aside from the above mentioned challenges of employing a data protection model based on consent and purpose limitation, the use of AI based applications also renders anonymisation an inadequate standard for protecting individual privacy. New research shows that data can be de-anonymised in a number of ways, particularly as data sets are combined. [4] Retaining data for a long period of time may also result in having a larger data pool. In these circumstances, there may be a risk that data that has been de-identified in isolation may be capable of re-identification when arranged and analysed as a part of a larger data set. It is also possible that AI can recreate identities, or minimally, can create portions of identities that were originally removed to protect against discrimination. For example, there have been cases where gender and name were removed from resumes in order to help protect discrimination, however the AI tool was able to pick up subtle nuances in language that allowed it to recreate the candidate's gender.[5] The purpose limitation principle of the PDP can also lead to tension with the necessity for AI to use all of the information available to learn. Paradoxically, by limiting certain data sets, AI may have bias introduced because it is only being trained on subsets of the dataset, instead of all available data.[6]

With big data analytics and machine learning, a whole range of inferences and correlations can be drawn, which could result in social sorting, discrimination, and surveillance, even for those who were not included in the data set. Big data analytics and AI draw inferences and predictions about the behaviours, preferences, and private lives of individuals. Often it is not the information that is collected in itself that is sensitive, but rather the inferences that are drawn and used that is sensitive and concerning. PDP as is currently imagined will fail to protect data subjects from the novel risks of inferential analytics. Counter intuitive and unpredictable inferences can be drawn by data controllers, without individuals ever being aware, thus posing risks to privacy, identity, reputation, and informational self-determination. Transparency and consent mechanisms designed to manage input data are no longer sufficient; there needs to be ways to have control over whether, how, inferences are made and used. Data protection needs to include a right to explanation and reasonable inferences as well.[7] Yet, it is also important to recognise that as the harms of AI extend beyond individual privacy, data protection frameworks will also be inadequate on their own.

4 Paul Ohm, 'Broken Promises of Privacy: Responding to The Surprising Failure of Anonymization' (2010) 57 UCLA Law Review 1701.

5 Jeffrey Dastin, 'Amazon scraps secret AI recruiting tool that showed bias against women' (Insight, 10 October 2018) <https://in.reuters.com/article/amazon-com-jobs-automation/insight-amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idINKCN1MK0AH> accessed 23 February 2020.

6 Amanda Branch, 'AI & Privacy: The Struggle is Real: meAnIngful consent and retAIning data' (Bereskin & Parr LLP, 29 August 2019) <https://www.lexology.com/library/detail.aspx?g=f3687556-098b-4d76-aa16-0e67462c2f4b> accessed 23 February 2020.

7 Sandra Wacter and Brent Mittelstadt, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' (2019) Columbia Business Law Review.

4. EXCESSIVE EXPANSIONS OF STATE POWER

The Bill does not provide adequate protections to citizens from government agencies. The Bill allows the central government to be exempt from the provisions of the bill, as well as gives it powers to exempt any government agency from the application of the Bill. This can lead to abuse and misuse of power by the state and unwarranted violations of privacy, particularly as the conditions under which this exception holds are hugely under-specified and open to multiple interpretations.

Of particular concern is the clause that allows government agencies exemptions for preventive purposes i.e. preventing any activity that could undermine the sovereignty and integrity of India, the security of the state, friendly relations and public order. The earlier version of the Bill granted that these exemptions would only be permitted through the passing of relevant law and passing principle of proportionality; this version significantly dilutes this safeguard to 'necessary and expedient', with this decision left to the government's discretion. In a discussion with Economic Times,[8] Justice BN Srikrishna, who headed the committee tasked with drafting the Personal Data Protection Bill, drew attention to this removal of safeguards, cautioning that it risks leading to the creation of an Orwellian state. The Bill also falls short of the standard developed by the Supreme Court in the Puttaswamy case[9] i.e. the measure must have a legitimate goal; the measure must be suitable for furthering the goals; it should not a less restrictive but equally effective alternative; and the measure must not have a disproportionate impact on the right holder. As recommended by the Srikrishna Committee, the access of personal data by Government agencies must be subject to judicial oversight.

The appointment of the DPA also points to a worrying centralisation of power. The DPA is currently to be appointed by the Central Government, which could severely undermine its independence and its credibility. The independence of the DPA will be essential to establish trust in the digital ecosystem. As in the previous version of the bill, the DPA should be constituted through judicial appointment, not through the Central Government. Building trust in the DPA is particularly important because of the the tensions between individual privacy and leveraging data for public good. A related concern regarding the centralisation of power is the authority granted to the central government for the notification of data as sensitive or critical personal data.

5. UNDUE EXCEPTIONS FOR SEARCH ENGINES

Search engines have consistently been the subject of debate. While they were earlier seen as mere facilitators of information, this understanding has changed

8 Megha Mandavia, 'Personal Data Protection Bill can turn India into 'Orwellian State': Justice BN Srikrishna' (Economic Times, 12 December 2019) <https://economictimes.indiatimes.com/news/economy/policy/personal-data-protection-bill-can-turn-india-into-orwellian-state-justice-bn-srikrishna/articleshow/72483355.cms?from=mdr> accessed on 23 February 2020.

9 Justice K. S. Puttaswamy (Retd.) and Anr. vs Union Of India And Ors.

drastically as search engines use algorithms to filter and prioritize content, personalised to users. This gives search engines access to an enormous amount of data about citizens, as well as curatorial power to shape how citizens know the world and are perceived by others. The exceptions given to search engines thus seem arbitrary and unwarranted. These exemptions require re-evaluation owing to the large amounts of personal and sensitive personal data collected and processed by search engines.

6. SOCIAL MEDIA VERIFICATION CAN UNDERMINE ANONYMITY AND SECURITY

The motivation behind the bills requirement that social media intermediaries allow users the option to verify themselves is unclear. There is no obvious reason this would help the spread of misinformation. Rather, it could undermine the anonymity, safety, and privacy of users, and enable surveillance. Further, it reads counter-productive to the purpose of data protection as it necessitates the collecting of more information from users .

CHAPTER WISE COMMENTS & SUGGESTIONS

1. DEFINITIONS

1.1. ANONYMIZATION

The bill states in Clause 91 that provisions of the act will not be applied to anonymised data, and any form of anonymization carried out must be according to standards set by the authority. However, the inherent risk of re-identification present in the practice of anonymization is now well-established.[10] New machine learning based applications are capable of re-identifying data by extracting relationships from seemingly unrelated data. In these circumstances, there may be a risk that data that has been de-identified in isolation may be capable of re-identification when arranged and analysed as part of a larger data set. Hence, this possibility of re-identification should also be included in the standards set by the Authority.

More importantly, the bill must acknowledge the occurrence of re-identification and adjust the language and the provisions of the bill accordingly. It would be useful to look the GDPR's approach as it accommodates for the fact that anonymization is no longer feasible; it identifies other risk based measures such as pseudonymisation, data protection impact assessments, measures of data protection by design and by default[11].

1.2. HARM

The bill defines harm in Clause 3(20)(x) as the result of particular actions, whether bodily injury or denial of a service, and includes in its definition any observation or surveillance that is to be reasonably expected. However, it is important to recognise that the very notion of a data protection framework that is largely reliant on the concept of 'harm' is likely to be inadequate. Certain actions could constitute privacy violations, even if there are no observable harms or consequences. These harms might manifest at a later day, and in ways that are not directly or obviously related to the privacy violation. This concept of harm essentially fails to recognise that the action in itself must also be accounted for; the underlying violation that has resulted in the harm thus receives no reprimand.[12]

[10] Paul Ohm, 'Broken Promises of Privacy: Responding to The Surprising Failure of Anonymization' (2010) 57 UCLA Law Review 1701.

[11] Mike Hintze, 'Viewing the GDPR through a De-Identification Lens: A Tool for Compliance, Clarification and Consistency' (2017) 1(1) International Data Protection Law 86.

[12] Jason R Cronk, 'Why privacy-risk analysis must not be harm focused' (IAPP, 15 January 2019) <https://iapp.org/news/a/why-privacy-risk-analysis-must-not-be-harm-focused/> accessed on 7 February 2020.

Further, in the context of emerging technologies like artificial intelligence and the internet of things, the notion of what constitutes a reasonable expectation of surveillance is problematic. Data is being collected from multiple sources, as varied as personal devices and traffic toll gates, and the combination of these data sets can create granular profiles of individuals. Individuals are thus unlikely to know when their data is being collected or combined and similarly unlikely to understand how their various digital interactions can contribute to their surveillance. It is necessary that a standard of reasonable expectation be set by the Bill, and restrictions be placed on the deployment of large scale invasive technologies.

1.3. PROCESSING

The definition of processing in Clause 3(31) is part of the most critical terminology in establishing a data protection framework, as it aims to regulate the processing of data. The provision defines processing of personal data as an operation or set of operations performed on personal data and may include operations such as collection, recording, organisation, structuring, storage, adaption, alteration, retrieval, use, alignment or combination, indexing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction. The Bill in its current form lacks explicit mention of automated decision-making which plays a major role in the processing of data; this adversely impacts the user rights by excluding safeguards against such processing.

2. OBLIGATIONS OF DATA FIDUCIARIES

2.1. LIMITATIONS OF NOTICE AND CONSENT FRAMEWORK, PARTICULARLY WITH BIG DATA AND AI

On consent, the expectation is that it should be free, informed, specific, clear, capable of being withdrawn and for a specific purpose. This is problematic for a number of reasons; proposals to improve and fortify notice-and-consent, such as clearer privacy policies and fairer information practices, will not overcome a fundamental flaw in the model, namely, its assumption that individuals can understand all facts relevant to true choice.Consent is often a not a choice, where withholding consent could result in the denial of essential services or exclusion from political, economic and social life. Low levels of level literacy, the complicated nature of terms and services, and consent fatigue reduce the possibility for informed consent. Digital companies not only collect personal data, they also process that data to create new information that does not belong to the original user, complicating consent further. Therefore, rather than focus on only improving notice and consent frameworks, we must articulate a backdrop of context-specific substantive norms that constrain what information websites can collect, with whom they can share it, and under what conditions it can be shared. We need to develop frameworks for legitimate collection and use, including conditions for the combining of data sets.

These problems are further exacerbated in the context of AI - because of the opaque nature of machine learning systems, it is not feasible to know the ways or purposes for which data is being used. AI exacerbates and exponentially multiplies the existing trends to over collect data and use data for

unintended purposes not disclosed to users at the time of collection. The more data collected the smarter, faster and more accurate the algorithms will be. There is an incentive to over collect and use data to develop algorithms to accomplish novel tasks. Therefore, a one time conclusive consent model might not be the most appropriate with regards to concerns at hand; experts have suggested moving to a model of continual and non-binary consent[13]. The Information Commissioner's office in the United Kingdom proposes a process of graduated consent as opposed to binary consent; the former essentially allows users to provide consent to different uses of their data throughout the use of services instead of a single option at the beginning[14]. This model might prove useful to the concerns raised with data minimisation, purpose limitation and AI; a continual requirement of well-informed consent will keep in check the volume and purpose for which data is being collected.

3. GROUNDS FOR PROCESSING PERSONAL DATA WITHOUT CONSENT

3.1. BROAD EXEMPTIONS FOR STATE

Clause 12 under the Bill sets out certain cases in which consent does not need to be obtained if processing of data is necessary in carrying out function of the State that are authorised by law for providing benefits and services or issuance of certification/license/permit for any activity. The terms 'service' or 'benefit' however are not defined in the bill, and could lead to a wide range of exceptions. This lack of clarity in the contents of the provision necessitates the incorporation of the principle of proportionality as per the Puttaswamy judgement, in addition to removing it from the exceptions to consent. If this limitation through proportionality is applied, it might work toward ensuring that not 'any function or service of the state' automatically allows for its application to 'every function and service of the state'. [15]

A significantly more concerning aspect of this provision lies in the subclauses (c) to (f) which involves processing for compliance with judicial processes, medical emergencies or even public disasters; these scenarios are more than likely to involve sensitive personal data and through this blanket exception provided by the provision it will result in the processing of such sensitive personal data without even the consent of the data principal, much less explicit consent. It is important that if the exemptions contain any likelihood of sensitive personal data being processed, it must be dealt with by the Bill separately and held to a much higher standard of protection.

13 E. Carolan, 'The continuing problems with online consent under the EU's emerging data protection principles', Computer Law & Security Review 32(3) 2016, pp. 462-473, 472.

14 ICO, 'Big data, artificial intelligence, machine learning and data protection' (Information Commissioner Office, 09 April 2017) <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf> accessed on 15 February 2020.

15 Justice K. S. Puttaswamy (Retd.) and Anr. vs Union Of India And Ors.

3.2. WEAK EMPLOYEE PROTECTIONS

The bill in Clause 13 provides an exemption to the condition of consent, if personal data is being processed for employment purposes such as recruitment/termination, provision of a service/benefit, verifying attendance or any other activity that might be related to assessing the performance of an employee of the data fiduciary. The motivation for this provision is unclear - employee data is already used without consent in a number of cases - instead of legitimating this practice, the bill should develop provisions that can enable protection reasonable to the nature of the relationship. The PDP should incorporate a safeguard against the misuse of employee personal data; this can be carried out by relying on the GDPR's principle of legitimate basis. The exemption to consent should be justifiable by the employer to employee that the processing was carried out, either for the performance of the contract, in complying with a legal obligation or in pursuance of the employer's legitimate interest. Additionally, as consent might not be an adequate requirement, it is important that, in keeping with the essence of a data protection framework, the Bill necessitates notifying employees of the use and purpose for use, of personal data collected and processed by their employers.

3.3. ARBITRARY LIST OF OTHER REASONABLE PURPOSES, PARTICULARLY THE INCLUSION OF SEARCH ENGINES

Apart from the other exemptions to consent provided in the Bill, Clause 14 allows for processing without consent to take place for certain reasonable purposes, of which one of them is for the operation of search engines under 14(2)(h). Reasonable purposes include a wide range of things but the rationale toward such inclusion is not clear; it appears to be a rather arbitrary list and the Bill must elaborate on the reasoning for these exemptions.

Specifically with regard to search engines, the Bill provides no reasoning for its inclusion as a reasonable purpose. As service providers to data principal's, search engines collect and process large amounts of data often through search histories of the user or through the form of cookies; this data can indicate behavioural patterns of the user amongst other sensitive personal information[16]. As content providers, it furthers accessibility of information; its 'representation and aggregation capabilities' allow it to crawl, analyse and index the internet in order to make all its information searchable by users.[17] This is sufficient to establish the need for search engines to require consent of data principal's in processing personal data. This has precedence in the EU, where even though search engines are covered by intermediary liability frameworks, these safe harbour provisions do not exempt them from compliance with data protection. It is for this reason that the Bill's moving away from conferring such responsibilities on search engines proves to be worrisome.

16 Working Party 29, Opinion 1/2008 on data protection issues related to search engines, WP 148, 04 April 2008.

17 ibid.

4. RIGHTS OF DATA PRINCIPAL

4.1. RIGHTS ARE INADEQUATE IN FACE OF AUTOMATED AND ALGORITHMIC DECISION MAKING

Right to access, as currently formulated in Clause 17, is inadequate as it does not take into account instances of automated and algorithmic decision making ('ADM'). In contrast, the GDPR can be read to have the right to explanation - this right in GDPR is derived from a combination of rights to access, notification requirements and safeguards against automated decision making. This right to explanation seeks to facilitate transparency and accountability around ADM and therefore, it would be beneficial to the data principal if ADM is included in the bill, and a related right of explanation. In this vein, it would be valuable to also incorporate the right to reasonable inferences. Additionally, the right to erasure and to be forgotten is made complicated in the context of new machine learning technologies, as individual data is used to generate new inferences and insights, that can continue to impact individuals even after the erasure of information. To ensure individuals are protected from discriminatory outcomes, in the pursuit of transparency and accountability, there is a need to be notified of ADM and be given the choice of opting out, particularly in public systems.

4.2. CONSENT MANAGER IS AN IMPORTANT BUT UNDERDEVELOPED IDEA

The Bill's introduction of a consent manager in Clause 21(1) and 23(3)(4)(5) could be a useful tool to provide users with better control over their data, but has been introduced without explanation. Though well-intentioned as it aims to beat the long-standing argument of consent fatigue[18], it fails to address the need of establishing security safeguards for such consent managers. The managers aim to provide users with a single platform to exercise all their rights; this raises concerns of the possibility of unauthorised access to these platforms. Further, there is no clarity on the manner in which the platforms will operate, retention of user data and even how such interoperability is to be achieved.

5. TRANSPARENCY & ACCOUNTABILITY MEASURES

5.1. NEED PRIVACY BY DEFAULT, NOT JUST DESIGN

The GDPR has provisions for ensuring both, privacy by design and privacy by default. Privacy by design refers to technical and organisational measures that ensure privacy is safeguarded right from start i.e. the early stages of design through measures such as pseudonymisation. Privacy by default, on the other hand, refers to default mechanisms (such as preferences or settings) that afford users the maximum amount of protection for their privacy from the get

[18] SFLC, 'Key changes in the Personal Data Protection Bill 2019 from the Srikrishna Committee Draft' (SFLC, 12 November 2019), <https://sflc.in/key-changes-personal-data-protection-bill-2019-srikrishna-committee-draft> accessed on 7 February 2020.

go. While the Bill does discuss an obligation on fiduciaries in Clause 22, to prepare a privacy by design policy, it is crucial that in alongside certification of the policy, the Authority ensure implementation of the policy also receives sufficient supervision, as it lacks mention in the Bill. Additionally, the inclusion of the principle of privacy by default as an obligation on data fiduciaries would help strengthen India's data protection framework.

5.2. DATA BREACH PROVISIONS GO AGAINST ESSENCE OF AFFORDING PROTECTION

The Bill in Clause 25 only necessitates notifying the Authority if the data breach is likely to cause harm to the principal; this is then assessed by the Authority in prescribing measures to mitigate the breach, and only after this is the Authority required to consider informing the data principal purely depending on either the severity of the breach or if the data principal is necessary in mitigating the breach. This goes against the very essence of affording protection to the data principal.

The Bill should necessitate that all personal data breaches be reported to the Authority, and not leave the subjective interpretation of harm to data fiduciaries. Further, more specification is needed of the conditions under which the Authority will not inform the data principal and the remedial measures that will be taken; without such specification, it is unwarranted that data principals are not notified of data breaches. The standard set by the GDPR in Article 34 with regards to providing notifications to the data principal, requires that data breaches that are likely to affect the rights of the data principal should be communicated unless it meets certain conditions. The Bill should look to incorporate a similar approach; the conditions listed by the GDPR prove to be appropriate and not too cumbersome for data fiduciaries if included. According to the Article, communication is not required if, firstly, the fiduciary had sufficient measures that were in place to protect the personal data and especially if the measures would ensure that access to this data would provide any benefit; secondly, if the fiduciary has taken measures to ensure there is no further risk to the principal and lastly, if the communication is not feasible, a public communication or measure is instead carried out which would inform the data principal.

5.3. SOCIAL MEDIA INTERMEDIARIES AND USER VERIFICATION

The Bill in Clause 26(4) and 28(3)(4) requires notifying data fiduciaries as significant data fiduciaries based on certain set out criteria. A new addition to this is found in a separate provision that identifies 'social media intermediaries'; this is brought within the ambit of significant data fiduciaries under two conditions, firstly, if they are notified by the Central Government and secondly, are likely to have a specific impact as listed by the provision. While the obligations of maintaining records, audits, appointment of data protection officers and conducting data protection impact assessments will bring large social media companies under necessary scrutiny, the need for a separate determination of these intermediaries appears to be excessive and unnecessary. As the obligations of a significant data fiduciary are already carved out, there is no clear rationale in specifically notifying social media intermediaries under this category.

Far more concerning is the new requirement by Clause 28(3) and (4), which requires that these social media intermediaries must make available to the users, based or accessing services in India, the voluntary option of verifying their accounts on the platform. This verification will provide the user with a 'demonstrable and visible mark' that will be visible to other users. The requirement of verification has no clear benefit in a data protection legislation.Instead, it reads counter-productive to the purpose of data protection as it necessitates the collecting of more information from users with no purpose whatsoever. The provision does not specify the manner or the data/information required from users to obtain such verification and neither does it discuss the manner of retention of such information.

Most importantly, it can be used to surveil and profile users, both those who have registered and those who are unregistered for verification. For those who have registered, with no safeguards in place, their information could be used against them in violation of their data protection rights[19]. Users that do not want to be part of this process, risk being flagged, and verification thereby becoming a soft-mandate on users. Further, if the motivation for this provision is to arrest the spread of information, it is unclear how this will be achieved through verification.

5.4. DATA PROTECTION IMPACT ASSESSMENT

Clause 27 of the Bill prevents significant data fiduciaries from processing personal data without conducting a data protection impact assessment if they intend to process personal data through the use of new technology, for large scale profiling, or if the sensitive personal data has risk of harm to the principal. This provision implicitly acknowledges the possibility of automated data processing and demonstrates the need to consider this across various provisions. It is thus important to provide safeguards to processing of data by way of affording sufficient rights and choices to the data principal to refuse certain types of processing.

Further, sub-clause (1) prohibits the commencement of processing before the assessment is carried out, however, sub-clause (5) states that after receipt of the assessment, the Authority might direct to cease processing or direct that it be done under certain conditions. The phrasing indicates that processing might occur prior to the assessment which contradicts sub-clause (5); it is critical that processing is only carried out post the assessment and receipt of approval from the Authority. The provision also introduces the concept of data auditors as certain individuals that have expertise in areas listed by the clause, however it would be useful to for assessments and audits to be carried out by more than one auditor, possibly by a larger group of auditors from various backgrounds.

19 Internet Freedom Foundation (IFF), 'A public brief and analysis on the Personal Data Protection Bill, 2019' (IFF, 25 January 2020) <https://saveourprivacy.in/media/all/Brief-PDP-Bill-25.12.2020.pdf> accessed on 7 February 2020.

5.5. DATA TRUST SCORES NEED TO BE DEVELOPED FURTHER

The Bill requires that significant data fiduciaries have their policies and conduct of processing data audited annually by an independent data auditor which will assign a data trust score. This is an important concept that could help shift the burden of responsibility away from the data principal, establish trust, and reduce information asymmetry between the data principal and data fiduciary. There, however, is no clarity as to the format of a data trust score or the manner in which it is to be calculated. As the concept is unseen in other data protection regimes, it is important that the Bill comprehensively address the introduction of a data trust score.

6. RESTRICTIONS ON TRANSFER OF PERSONAL DATA OUTSIDE INDIA

6.1. ARBITRARY NOTIFICATIONS AROUND PROCESSING AND STORAGE OF SENSITIVE PERSONAL DATA & CRITICAL PERSONAL DATA

The localisation requirements as set out by the previous draft of the Bill has been diluted, mandating the storage of personal sensitive data in India, but allowing for processing outside India with the explicit consent of the data principal. While this is welcome improvement from the previous bill, to enable citizens with greater control over their data, the provision still requires authorisation by the Central Government for such processing, and thus curtails citizen rights. While we acknowledge the need for keeping a copy of the data stored in India for law enforcement purposes and cumbersome bureaucratic procedures entailed in access citizen data stored elsewhere, the decision around processing should be with citizens. The previous draft of the Bill empowered only the Authority with the power to determine additional categories of sensitive personal data. The current Bill, however, provides the Central Government the primary power to notify these categories and requires it to do so only in consultation with the Authority. This risks the subordination of this process to short term political goals and political contestation. The Bill further states that all critical personal data must be stored and processed in India, but leaves it to the discretion of the government to decide what constitutes critical personal data; it further does not provide any guidelines or specifications on how this notification is to be made. This can lead to the arbitrary or politically motivated notification of critical personal data, resulting in the restriction of privacy and other rights.

7. EXEMPTIONS

7.1. EXCEPTIONS TO CENTRAL GOVERNMENT CAN LEAD TO UNCHECKED COLLECTION AND USE OF DATA

Clause 35 permits the Central Government to exempt any agency of the Government from the application of the provisions of this Bill, if in the interest of sovereignty and integrity of India, security of the State, public order, friendly relations with foreign states or to prevent the incitement to the commission of offences. Clause 36 affords exemptions to processing of personal data in the interests of actions toward offences, legal rights, in exercising of judicial

function or professional activity.

This is a glaring departure from the 2018 draft bill that mandated this exemption be permitted pursuant only to a law made by Parliament, through the procedure laid down by such law, and as long as it was necessary and proportionate. The current Bill substantially dilutes this safeguard, empowering the Central Government to exempt itself and its agencies through only the passing of an executive order as long as it's 'expedient and necessary'. Additionally, the conditions for the exemptions have also been widened from the earlier sole criteria of 'security of the State' to event preventive action in the name of public order, enabling thereby a range of situations that could be afforded an exemption. The core fear that arises out of this is the free reign given to the Government to be the arbiter of its own actions with no accountability over its ability to exempt itself and its agencies from the provisions of the Bill. The lack of any judicial oversight combined with burgeoning technology capable of establishing a mass surveillance regime will negate the very purpose of enacting a data protection framework.

Similarly, the 2018 draft Bill's requirement that exemptions provided under Clause 36 be subject to a law made by Parliament and State Legislature that was necessary and proportionate, is no longer part of the 2019 Bill. Lack of accountability, especially in the processing of personal data with regard to offences can contribute to the unbridled power afforded to the Central Government in conjunction with exemptions provided under Clause 35.

7.2. SANDBOX FOR ENCOURAGING INNOVATION

Clause 40 of the bill enables the Authority to create a 'Sandbox' for data fiduciaries, for the purposes of encouraging innovation in artificial intelligence, machine learning or any other emerging technology, in public interest. In furtherance of that objective, the clause provides actors whose privacy by design policy has been certified by the Authority an exemption/relaxation from certain obligations for a period of 3 years.
Sandboxes allow for better dialogue between the regulators and stakeholders and enable a hands-on assessment of risks involved in innovation, and while this move may help develop better regulation, it also presents a host of challenges. The provision is vague on what constitutes innovation or public interest. Further, there is a lack of clarity on qualification processes and what regulations shall govern the functioning of the sandbox. The Bill also requires the Authority to certify the privacy by design policies of not only fiduciaries selected for the sandbox but instead maintains this requirement as a prerequisite to qualify for inclusion, which is more than likely to lead to a very overburdened Authority[20]. The assessing of the privacy by design policies should instead come after an initial round of selections based on meeting the objectives and purpose of the sandbox.

20 Smriti Parsheera, 'Regulatory governance under the PDP Bill: A powership ship with an unchecked captain?' (Medianama, 7 January 2020) <https://www.medianama.com/2020/01/223-pdp-bill-2019-data-protection-authority/> accessed on 10 February 2020.

From a data protection sandbox perspective, a useful example is the United Kingdom's Information Commissioner's Office (ICO), which opened a phase of its regulatory sandbox scheme in 2019. Through this, it supports organisations that intend to use personal data in order to develop innovative and beneficial projects; however, the ICO approaches this sandbox differently from the Bill. It does not provide a carte blanche to these organisations. Instead, it works with these organisations in developing a manner of compliance with data protection laws. Further, it would be worth considering the implementation of a similar approach as carried out by the ICO and restricting the number of fiduciaries selected as part of the sandbox; this will ease the load of the Authority and ensure sufficient space for engagement between the Authority and the fiduciaries.

8. DATA PROTECTION AUTHORITY

8.1. PROPOSED APPOINTMENT STRUCTURE AND FUNCTIONING LACKS INDEPENDENCE

The Data Protection Authority referred to throughout the Bill is to be appointed by the Central Government based on recommendations provided by a 'selection committee' under Clause 42; Clause 86 affords the Central Government the final power in issuing binding directions to the Authority. Any diversity in the composition of the appointment committee as prescribed in the 2018 draft Bill has been replaced purely with members of the Government and through these provisions the increasing shift of power toward the executive appears to be more apparent. It is critical that the independence of the Data Protection Authority is preserved, therefore the control of the Central Government over composition of the selection committee and in the power it has to issue final directions must be re-evaluated.

9. MISCELLANEOUS

9.1. PROVISION FOR NON PERSONAL DATA IS UNFOUNDED, SUBSUMING PRIVACY TO ECONOMIC GROWTH OBJECTIVES

The formulation of a data protection framework should be driven by the aim of affording the data principal the highest of privacy measures and as a result should not be founded on sovereignty, economic development and regulatory access unless it is contributing to the protection of data through it.[21] In this light, it would not be in the interest of the data principal for the Bill to deal with the use of non-personal data.

Moreover, the further concern with the Clause 91(1),(2) is its deep reliance on anonymisation; reiterating that the re-identification of anonymised data has been acknowledged by numerous experts in the field to be more than likely, it would be beneficial to err on the side of caution in providing the

[21] National Institute of Public Finances & Policy (NIPFP), Comments on the Personal Data Protection Bill, 2018' (NIPFP, 10 October 2018) <https://www.medianama.com/wp-content/uploads/NIPFP-Submission-India-Draft-Data-Protection-Bill-Privacy-2018.pdf> accessed on 7 February 2020.

Government with an all pass access to anonymised data. Therefore, it would be recommended that the additional risk-based measures as recognised by the GDPR. Further, with the various rapidly developing forms of technology, it is becoming increasingly difficult to draw a clear distinction between personal and non personal data; even seemingly non-personal data can alter social systems in which people are embedded, and thus impacted.

Tandem Research
343 Coimavaddo Quitla, Aldona
Goa - 403508
www.tandemresearch.org