Solving for data justice: A response to the draft Personal Data Protection Bill
Submission by Concerned People
10 October 2018

In late July 2018, the B N Srikrishna Committee, instituted by the Government of India for this very purpose, released a draft Personal Data Protection Bill and report.

The starting point of the draft Bill and report is an understanding of data as a resource to be tapped. But other perspectives on data, encapsulated in alternative metaphors, exist, some of which are much better at foregrounding the interests of data principals than the widely used metaphor of data as oil. Data often is also an extension of our bodies, though it can turn into exhaust, even pollution. Data can be the key to unlock recognition, but can also function as a distraction, or propaganda. Data is widely monetised, but when it is understood as the product of labour, this raises questions about who it is enriching. More data does not necessarily mean more insight, then, just more raw material for interpretation.

These alternative perspectives, though deeply representative of our experiences, are largely absent from the draft Bill. As concerned people with a wide range of backgrounds and interests and rooted in various social movements, it is precisely these alternative lenses that we have brought to our reading of the draft Bill. The draft Bill's stated aim is to put forward a fourth way in data protection, tailored to the realities of India and other developing countries. But by ignoring these perspectives, we maintain, the draft Bill also completely disregards many of the realities of power, knowledge, subjectivity, inequality and capital flow in the Indian context.

We submit to you more detailed comments to substantiate this claim below, in four broad categories. At present, it deserves to be noted, as the outlook of the Bill does not represent the perspectives noted above, our comments are necessarily broad in many places. We will, however, be happy to provide section-wise comments on a future draft of the Bill that has broadened to include these insights. As the issue under discussion in this Bill deeply affects every single Indian, we also request that the next draft Bill be released in multiple Indian languages besides English. Only then will a genuinely broad-based public consultation be possible.

The Puttaswamy judgment of 2017 recognised that the right to privacy is essential to the autonomy and dignity of people. While consent alone may not be able to lift this weight (more on this below), it remains a crucial mechanism through which to ensure the individual's autonomy and dignity is respected. The draft Bill fails in this respect.

1. **Although the report recognises the normative value of consent, in the Bill consent effectively is reduced to a mechanism through which private companies are able to escape liability for harm.** In the context of, for example, sexual rights, where consent has perhaps found the richest conceptual development till date, the function of consent is not merely to prevent harm, but to guarantee pleasure. If such a substantive understanding of the concept of consent is translated to the field of

privacy protection, it would thus be used not merely to prevent harm, but to ensure the will and interest of the citizen as a rights-bearing subject has been respected. In fact, the etymological meaning is 'of the same mind'. It is the duty of the State to ensure that an architecture that enables this is in place, both in the relationships that citizens have to the State, and in the relationships that they have with other entities. Focusing only on the avoidance of liability for harm, this draft Bill fails in that duty.

2. **Purpose limitation should be narrower. In addition to a far more narrow definition of purpose limitation, data minimisation should be introduced into the Bill.** As we know from debates about sexual rights, consent is not static, but dynamic. For consent to be meaningful, it has to be negotiable. Without options, where you can consent to *this* part but not *that* part, consent is at best a facade. In addition, for a valid choice to occur, it is essential that you have all the information you need. Consent without having been fully informed about how your data will be used amounts not to consent, but to manipulation at best and blackmail or coercion at worst. For these reasons, consent is best required incrementally. In other words, only narrowly defined purposes and minimal data collection enable meaningful consent at each stage of the relationship between a data principal and a data fiduciary.

3. **Consent should allow data subjects to hold data fiduciaries accountable.** Consent must be constantly created by a continuous flow of information and transparency: much like the State itself allows for the re-evaluation of our consent to the government by elections and free speech/press, similar mechanisms must be created in the relationship between data principals and data fiduciaries.
   The proposed framework, while requiring stronger commitments for notice and for demonstrating compliance, falters in this as it allows data fiduciaries to sidestep consent by allowing broad grounds for processing by the State and wide room in the grounds under reasonable purposes. Acquiring a full copy of information available with the data fiduciary under the right to access and correction, as well as a right to subsequently erase that information, are some of the concrete ways in which consent can be strengthened by improving transparency.
   With impediments to a transparent flow of information, operationalisation of meaningful consent is affected, leading to a fragmentation at various levels - whether of literacies, identities, and other intersectionalities. This in turn leads to widening social disparities. The Bill should enshrine consent that is based on transparent information, and thus is effective in ensuring accountability, leading to inclusive citizen participation.

4. **Design choices that promote intentional, narrow and informed consent should be incentivised.**

5. **If legal consequences for the effects of withdrawal are to be borne by the data principal, the value of the ability to withdraw drastically falls.** For consent to be meaningful, withdrawing it has to be a realistic option. The Bill leaves the user without a clean exit, while leaving further space for manipulation of users by those

seeking consent. The ease of withdrawal of consent should be comparable to the ease with which consent was taken.

6. **Replacement of minors' consent by their parents consent should be struck and teenagers should be allowed to provide consent themselves.** Replacement of minors' consent by parental consent does not reflect social realities, as many young people support their parents in navigating the online, rather than the reverse. Imposing parental consent in this context does not account for peculiarities of technological literacy in India.
   Moreover, many young people try to keep data from their parents with good reason. For example, in the case of intercaste relationships, especially where family violence has occured, the interests of parents are often not aligned with the agency of young adults. In the case of transgender persons, parents often come in the way of the recognition of their gender identity. When minors are not allowed the privacy and individuality to declare their chosen personhood in their data, this could then lead to the exacerbation of dysphoria, mental ill-health, and even suicides. Acknowledging this reality is in consonance with the ideas embedded in the NALSA judgement, which recognised the rights of transgender persons.
   Recognition of minors' control over their data is therefore imperative.

In the age of 'big data' and algorithmic decision making, consent alone will never be sufficient to ensure that the autonomy, dignity and privacy of the individual, or collective interests for that matter, are protected. While the draft Bill aims to 'unlock the digital economy', without efforts for redistribution of the fruits of such an economy, data principals will continue to be subjects of data extractivism, whose information and data produce far more value for the State and the private sector than it does for citizens. However, the draft Bill effectively leaves the inequalities and injustices of the age of large-scale data processing unaddressed.

7. **The draft Bill skips vesting the rights required to address the power imbalance between data principals and what is called 'artificial intelligence' and 'big data' processing.** As the Indian government increasingly seeks to govern through databases and algorithmic decision making, and is encouraging private sector efforts in this direction as well, the absence in the draft Bill of rights for data principals that bring about transparency, accountability, choice and equity is a shocking omission. Rights such as a *right to explanation*, or to demand the logic behind a certain algorithmic decision, are imperative for a charter of rights that seeks to address the problems of our times.
   Such measures are particularly important to prevent the blackboxing of political processes through 'big data' and 'AI'. This blackboxing puts at particular risk those belonging to marginalised communities, who may moreover lack the skills, capacity or means to engage with new forms of digital interactions (for example laptops, mobile phones), or may not have a choice within the current digital ecosystem (for example welfare benefits distribution system through the biometrics based Aadhaar), further perpetuating their marginalisation.

8. **In light of the Puttaswamy judgment of 2018, as Aadhaar numbers will continue to act as unique identifiers that catalyse and enable profiling, a right to object to profiling, especially where such profiling can have legal or similar effects, is absolutely necessary and should be included.** This, too, is of importance to protect the rights of vulnerable and marginalised communities in particular. Although the majority judgment does not go so far as to recognise how Aadhaar numbers and the ecosystem itself is a classic enabler of profiling, it does recognise that profiling is dangerous. The minority judgment or the dissent in the case, by Justice D Y Chandrachud, acknowledges the inherent problem in gathering sensitive data on such a large scale.

9. **Instead, the draft Bill allows for overly broad grounds for processing (Sections 13-21) as well as exemptions (Sections 42-48) that not only undermine and defeat the impact of a consent-based framework, but that militate against the primary purpose of the law, which is privacy protection.** For example, employment as one of the grounds for processing data leaves wide room for exploitation by employers, and should be circumscribed. By allowing for processing in the 'public interest' as well as processing of publicly available personal data under Section 17, the draft Bill constructs the State's relationship to data in a way similar to the State's relationship to land and resources. If the doctrine of eminent domain has any lessons, it is that the meaning of 'public purpose' and related concepts should be very carefully examined. Public interest should therefore be clearly and narrowly defined in the Bill, while the processing of publicly available personal data should be made subject to the data principals' consent. Data Protection Impact Assessments should be required in both cases, as the Bill itself rightly defines harm in a broad way, including, for example, chilling effect to speech and expression (Section 3(21)).

10. **In making 'functions of the State' a ground for processing in particular, the bill leaves tremendous room for State entities to collect unsolicited data and process it, without empowering citizens to seek accountability for the same welfare delivery.** The bill and the wide leg-room the State demands through this particular ground must be seen in light of the gradual withdrawal of State from education, healthcare and other State functions. If this data grab in the name of welfare delivery is seen alongside State failure to deliver benefits, as evident with Aadhaar, it is clear that we need a reassessment of this ground. Clearly, more data does not necessarily translate into better policy.
    'Functions of the State' should therefore be more precisely and narrowly defined, and legal provisions and remedies to address misuse, if and when it occurs, should be addressed in the Bill. Further, data protection obligations under Chapter II, such as maintaining data quality by ensuring that records are updated in a timely manner wherever required, should apply equally to processing of personal data for State function.

11. **As the environmental rights movement has taught us before, numerous vague or imprecise elements in the draft Bill make it likely that, when a simplistic formula is applied balancing the privacy interests of data principles against economic**

incentives, serious compromise in favour of the latter is likely. Consider an analogous balancing formula adopted by courts and the executive in balancing the needs of the economy and environment. It has repeatedly resulted in environmental interest finally being sacrificed. This will inevitably continue to happen unless we have a strong version of sustainable development that positively affirms that some environmental interests are non-negotiable and cannot be balanced against economic interests. Similarly in the draft bill, the overall reliance on the poorly defined/clarified standard of 'fair and reasonable', broad ill-defined exemptions, broad grounds of processing that can disregard consent, and poor clarity on what exactly terms like 'proportional' and 'necessary' mean when an individual's rights are implicated, in the likelihood of the scales tipping in favour of big corporations and the surveillance state.

12. **Rights drawing from anti-discrimination law should do the work of protecting vulnerable persons in the context of large scale data processing as well, and uphold the history of transformative constitutionalism embodied by, among others, the recent judgment reading down Section 377 of the Indian Penal Code.** When large-scale data processing takes place without a guarantee of legal safeguards against the risk of discriminatory outcomes and uses, it further empowers the State, in particular, to act with impunity - and this not only vis-a-vis targeted individuals, but also vis-a-vis marginalised communities, including around the matter of the legal status of different vulnerable communities. In anti-discrimination jurisprudence, the recognition of sex, caste etc. has not meant just similitude; rather the difference of social positions - including caste, religion, disability, sexual orientation and self-identified gender - has informed judgment of what equality would mean before the law, including an acknowledgement of the need for measures specifically aimed at safeguarding the interests of particular communities.

13. **Overall, the notion of sovereignty that is presented in the bill merely serves to amplify State power, without bringing any real relief to citizens from the kinds of digital colonialism that actually matter.** What is needed is decolonisation from values like technological solutionism and phenomena like surveillance capitalism. Instead of any meaningful change on those fronts, by requiring across-the-board data localisation and wide State exemptions for processing of data, the State acts as a benevolent patriarch who can do no wrong.

14. **It is a huge blow to transparency that data fiduciaries or the Data Protection Authority are under no obligation to make Data Protection Impact Assessments public.** The bill presently allows for unfettered large scale data processing under many grounds and exemptions, but does not create mechanisms or opportunities for feedback by data principals on desirability, room for bias and potential or actual harm. Space for independent reviews by citizens of Data Protection Impact Assessments should also be created under the Bill.

15. **Data Protection Impact Assessments should consider the cumulative and strategic aspects of the technology/project in question.** Environment impact assessment

(EIA) law and policy in India (per Supreme Court and National Green Tribunal jurisprudence and National Environment Policy) and across the world recognize the ideas of a) cumulative environment impact assessment; and b) strategic environment impact assessment. Cumulative impact assessment means that the additive, synergistic, and connected impacts of multiple projects or processes also feature in the EIA process. A Strategic EIA approach means that broader policies and programs (instead of mere projects) are also required to carry out impact assessments with built in process safeguards of scoping, public consultation, mitigation measures, consideration of alternatives, etc. Given the nature of data - particularly large-scale data processing and automated decision making systems - and how this might impact on the privacy rights of individuals, it becomes very important for impact assessments in the context of informational privacy to explicitly adopt and require both cumulative impact assessment and strategic impact assessment frameworks and norms.

The draft Bill misses the opportunity to specify procedures for law enforcement use of data. By providing sweeping exemptions for purposes of Security of the State etc., the bill legitimises dangerous trends that combine data, policing and broad State surveillance without safeguards for due process in place.

16. **The exemption for 'prevention, detection, investigation and prosecution of contraventions of law' is overbroad and insofar as it seeks to *prevent* commission of offences, brings the risk of amplification of biases embedded in criminal justice systems.** This ground of exemption alters the doctrine of citizenship itself, to treat all data principals as suspects first, and not as holders of rights. It also leads to the creation of a nanny state, where the dignity of risk is no longer allowed to citizens.

17. **Strong procedures for processing of data by the government for law enforcement purposes should be specified in the Bill.** The exemptions under Section 42 and 43 only require that they function pursuant to a law, and that they are 'necessary and proportionate' to the interests stated. This is not enough. The approval for each instance of exemption should go through a judicial process, and in a manner that allows for Parliamentary oversight periodically. It is useful to recall that the constitution bench of the Supreme Court struck down the national security exception in the Aadhaar Act as unconstitutional.
However, even where procedural safeguards have existed, recent history of government surveillance across the world tells us that these procedures are blatantly flouted. Especially in the absence of an environment of trust surrounding government handling of citizens' data, it is imperative that strict silos in government agencies' holding of data is required by law, and trust is built through strong implementation in good faith.

18. **The law expects private entities like Facebook and Google to notify data principals if data being collected will be shared with other entities, along with specifying the purpose. The same standard should hold for government.** There should be transparency about what data is held by which agency. In addition, if the health

department, for example, can share data with the police, the citizen should be notified of the possibility. As the history of HIV/AIDS activism, for example, has illustrated, where access to State benefits is conditional on disclosure of data, this frequently leads to people not availing of services they have a right to and instead turning to informal, underground channels. Acting upon this insight, the National AIDS Control Organisation decided not to make access conditional on disclosure; HIV/AIDS prevention would have suffered greatly if disclosure had been made a condition. Any data sharing should also happen only after the strengthened data protection obligations and procedural safeguards proposed in this submission have been put in place.

19. **Data localisation requirements exponentially increase the surface area available for existing surveillance programs.** Such a move disturbs the value that inheres in the current configuration of internet infrastructure. By requiring data localisation, the value that an open and secure internet brings, including the right to freedom of speech, expression and assembly, is under attack, while the surface area for State surveillance, especially in the absence of procedural safeguards, exponentially increases.

20. **It deserves to be noted that the ecological impact of data localisation requirement has been blissfully ignored.** Proponents of data localisation have argued for subsidised land acquisition and power supply, tax breaks and other incentives for stimulating data centers to be set up in the country.[1] Whether or not those exact measures are undertaken, the ecological cost does not even make its way into the cost-benefit analysis. This includes the high cost of keeping data centers at a stable, low temperature, even in the face of the energy crises that so many states are already facing. This is symptomatic of treating issues of tech policy in isolation from the other ongoing challenges in the country.

Finally, the Data Protection Authority should be independent and resilient, if the framework needs to be effective. A strong, independent Data Protection Authority that lends its ear not only to government and business, but also to citizens on an ongoing basis is essential to the implementation of any effective data protection framework. The Data Protection Authority should work to promote and protect citizens' rights. Here, too, the draft Bill falters.

21. **The draft Bill continues to be silent on many areas, insisting that they will be clarified by rules, regulations, codes of practice, and Data Protection Authority guidance in the future - but if the environmental story is anything to go by, there is a serious risk that the Data Protection Bill in its current version would get weakened through the backdoor of delegated legislation.** Drawing from Environmental Impact Assessment law and policy in India, we have seen that a reasonably strong initial environment protection framework (Environmental Impact

[1] Goenka, (August, 2018), Data Sovereignty - Economic Implications for the Country, *Business World*, http://www.businessworld.in/article/Data-Sovereignty-Economic-Implications-For-The-Country/28-08-2018-158649/.

Assessment Notification 2006) can get repeatedly and seriously weakened and diluted by a large number of changes that were subsequently introduced through government orders, bylaws and exemptions brought about through delegated legislation. Such a risk is particularly grave in the context of data protection, given the power imbalance between the government and big corporations on the one hand and individuals whose privacy rights are implicated on the other.

22. **The powers of the Data Protection Authority should be circumscribed, at the same time as curbs on its independence should be removed.** The Authority is empowered to add conditional grounds of processing of personal data. This is not acceptable. Further, in its present form, the Central Government can issue directions to the Authority which are binding, according to Section 98 of the Act. Such a compromise on the Authority's independence should not be accepted.

23. **The Authority should be required to conduct open and transparent consultation processes before a change in, or introduction of new policies.** The processes followed by TRAI could be used as a model.

24. **The Authority should necessarily have representation from amongst minority groups. Additionally, an advisory body consisting of gender and sexuality, caste, and regional minorities should be instituted to advise the Authority.** The Authority must have people who can represent the interests of data principals, like in the Mental Health Care Act, 2017, which makes room for representation of persons with mental illnesses as well as caregivers to be on the Central Mental Health Authority. In addition, mechanisms should be created - even if incrementally - to assist persons with limited digital literacy, to make representations to the Authority.

25. **Data principals should be informed in case of personal data breaches.** This should be the case not only for breaches by private entities but also extend to data breaches by the government. Non-disclosure as the default affects the relationship of trust that the draft Bill encourages between data principals and data fiduciaries. Where a data principal is not informed of a data breach, it will also be difficult for them to make the link with any harm they may be experiencing and thus to seek recourse.

Signed (in alphabetical order):

Abhayraj Naik, independent researcher
Aiswarya Jayamohan, Internet Democracy Project
Amba Salelkar, Equals Centre for Promotion of Social Justice
Amrita Sarkar, SAATHII
Anja Kovacs, Internet Democracy Project
Anubha Singh
Arpitha Kodiveri, Doctoral researcher at the European University Institute
Bishakha Datta, Point of View
Chanda Vajane,Veshya Anyay Mukti Parishad (VAMP), Sangli
Dhamini Ratnam, journalist
Kalyani Menon-Sen, Feminist Learning Partnerships, Gurgaon
Khetrimayum Monish Singh
Kishor Govinda, scientist and activist
Maansi Verma, legislative and policy researcher
Madhuresh Kumar, National Convener, NAPM Delhi
meena saraswathi seshu, SANGRAM, Sangli
Mythri Prasad-Aleyamma, Institute for Human Development
Nachiket Udupa
Namita Aavriti
Nayantara Ranganathan, Internet Democracy Project
Niveditha Menon, Bangalore
Padmini Ray Murray, digital humanities researcher
Pranjal Jain, Srishti Institute of Arts, Design and Technology
Rajendra Naik, MITRA Collective, Sangli
Rajendra (Sudhir) Patil, Muskan Sanstha, Sangli
Rajesh Umadevi Srinivas, Sangama
Shahin Makandar, Nazariya Collective, Sangli
Shreya Ila Anasuya, Writer and Editor, Skin Stories, Point of View
Siddharth Narrain, lawyer and legal researcher, Delhi
Srinidhi Raghavan, activist, writer and researcher
Sulbha Howale, Vidrohi Mahila Manch, Sangli
Thejesh GN, DataMeet
Vidya Viswanathan, Centre for Policy Research
Vinay K Sreenivasa, Alternative Law Forum, Bangalore