internet democracy project

The Internet Democracy Project welcomes the consultation by the Ministry of Electronics and Information and Technology on the draft personal data protection bill ("draft Bill"). We hope that responses will be made public in the interest of a transparent process.

In this submission, we note general concerns in the report and draft Bill and then address issues under each chapter of the draft Bill.

1. The draft Bill has introduced several important features, but seen together, it does not translate into a legislation that succeeds in shifting the power imbalance in favour of individuals and vesting citizens with the rights needed, considering the complexity and obscurity of data flows and business models, and the State's own ambitions of governance through data.

2. The right to informational privacy is integral to human dignity and autonomy, as confirmed by the plurality judgment in the Puttaswamy (2017) judgment. In the context of a data protection bill, it would be operationalised through control over data, the autonomy to decide how and where it may be used and by whom. The draft Bill does not succeed in vesting such control with data principals.

3. The 'gains' emerging from what is called the digital economy are in large part due to the phenomenon of surveillance capitalism and the enabling infrastructure for the targeted advertising industry. To address the worst excesses of data monetisation in the digital economy means to have to tackle these issues. Looking at the draft Bill, it is clear that most of these thorny issues will not see any chance of being addressed if the bill is passed in its current shape. The unambiguous espousal of the use of personal data for prevention of contravention of law (Sections 17(2)(a) and 43) and of profiling for scoring (Section 17(2)(e)), as well as the absence of rights against profiling and automated decision-making contribute to the draft Bill's inability to fully respond to some of these sticky issues in the digital economy.

4. Many of our misgivings about the draft Bill and report are due to a lack of conceptual clarity in the report. Crucially, the report conflates "collective values" with the limited restrictions to the right to privacy, in the plurality judgment in the Puttaswamy case (2017), and thereafter with legitimate interests of the State. Indeed, some restrictions

placed by the State in certain circumstances can arguably be in collective interest. However, "collective values" and "common good" are not interchangeable with ease of data sharing within the Government. The interests of data principals and the State do not always align, and indeed, the report itself recognises that it is safe to proceed on the assumption that the State is prone to excess. And yet, the report makes these slippages in multiple cases. This conflation forms the basis of wide State exemptions and grounds for processing for the State, which is one of the main problems with the draft Bill.

The report states that it is the understanding of the drafting committee that the State has a duty to put in place a data protection framework that, while protecting citizens from the dangers to informational privacy originating from State and non-State actors, serves the common good. The draft Bill fails in protecting citizens from dangers arising from State actors, does not go far enough in protecting citizens from non-State actors and conflates 'common good' with State prerogatives.

5. Far too many definitions, categories and procedures are left to be clarified at a later stage, either through delegated legislation by the Data Protection Authority or through interpretation. Given the amount of power that the government holds in the appointment of the various wings and the continued functioning of the Authority, later stage clarification of ambiguities is a huge concern.

Following are chapter-wise suggestions in addition to the main comments above.

Chapter I: Preliminary

- In addition to the application of the draft Bill to personal data, the draft Bill should also apply to non-personal data in certain cases, for example, where such data is being used to draw inferences about a group. Even if no personally identifiable information is processed, if the result of the processing is that there is group profiling that may impact persons of a particular group, there should be provisions made for data principals to exercise control in these situations under the draft Bill.

- 'Disability' should be included as one of the categories of sensitive personal data under Section 3(35), even though such information might separately fall under health data under Section 3(22) of the draft Bill. If the grounds have been identified on the basis of the kinds of information that might put data principals at a risk of greater harm than personally identifiable information would, then physical and mental disabilities are one such type of data.

- The breadth of 'financial data' under Section Section 3(19) should be expanded to bring transaction information within its ambit. High-volume transaction information gathered by fintech and other companies have a lot of value, as well as a lot of potential for harm. It should be protected accordingly.

Chapter II: Data Protection Obligations

- The general obligation under Section 4 that data fiduciaries process personal data of data principals in a 'fair and reasonable' manner as a normative standard is vague, and does not provide sufficient safeguards to data principals. Apart from being vague, this is a highly subjective standard applied in the context of data protection, as one person's sense of what is fair and reasonable does not correspond to another person's sense. One's determination of what might be 'fair and reasonable' would also depend on their social and political location in society, rendering this standard hard to apply. To take the example of an incident in recent public memory, what constitutes harm in mind of an important public official with dominant caste, gender and class identity when his phone number and address was revealed, was different from that of many women, trans persons and gender non-conforming persons, for whom the revealing of such personal information can have a range of harmful consequences.

- The criteria that are used to determine the purpose of processing under Section 5(1) (clear, specific and lawful) are weakened by the standard of reasonable expectation that follows in Section 5(2). What is reasonably expected today is necessarily shaped by the absence of any regulation around data processing for several decades, so does not serve as a useful circumscribing accompaniment.

- In addition to purpose and collection limitation, 'data minimisation' should be one of the features introduced into the draft Bill. It is the general principle that one should use the minimum amount of data to fulfil a particular purpose. This principle should be included to create an obligation to ensure that the personal data sought to be collected for processing is in fact indispensable for the activity in question.

- The detailed fields of information to be supplied under the notice requirement in Section 8 are a good measure. However, notice would continue to put a large cognitive burden on data principals. Solutions for operationalising notice should be given more attention.

- Notice requirements under Section 8 should apply to government processing of personal data as well. Clear information about how the State processes information for carrying out its functions is the first step in making the State transparent and accountable. Section 8(1)(e) specifies that the basis of processing and the consequences of the failure to provide such personal data be notified when processing of personal data is based on grounds from Section 12 to 17 and sensitive personal data from Section 18 to 22. This is absolutely necessary; however, it is unclear why the various ground have only been mentioned under Section 8(1)(e), when it should be applicable across all the different sub-sections.

Chapter III: Grounds for processing of personal data

- We appreciate that the normative value of consent is acknowledged. We recognise that it cannot be the sole feature on which the empowerment of data principal rests. However, it currently is undermined by the other wide grounds of processing, among other things.

- Consent withdrawal under Section 12 should be meaningful. If all legal consequences of the withdrawal are to be borne by the data principal, even where, say for example, the purpose of processing is altered and notice given, this puts the data principal in a position of powerlessness.

- Section 13, or the processing of personal data for the functions of the State is so broad that it undermines the purpose of the draft Bill. As a lot of the processing functions of the State are done in partnership with private companies, holding them to a different standard than data fiduciaries processing in a non-State capacity would shortchange the latter as well as harm citizens. Even if Section 37 were to limit what data processors can do with the data shared by a data fiduciary under a contract, this broad ground is still a concern.

- Section 15, or processing of personal data necessary for prompt action, can be done on the ground of 'breakdown of public order' - a broad ground which is ripe for interpretation. As internet shutdowns in the country have have shown, similar mandates to tackle public emergencies and ensure public safety have generally been construed in the service of censorship and stifling of dissent, among other ends.[1]

- The ground for processing of personal data for purposes related to employment is too broad, allowing for increasingly intrusive workplace surveillance methods. Particularly, Section 16 (1)(d) which allows processing if it is 'necessary' for 'any other activity relating to the assessment of the performance of the data principal who is an employee of the data fiduciary', allows many kinds of surveillance to thrive, including profiling on the basis of social skills, personal circumstances etc. Section 16 (1)(d) should be omitted.

- Processing of personal data for reasonable purposes is also overbroad. Where 'necessary' and 'public purpose' have not been better defined, this ground can end up leaving far too much room. In addition to narrow and clear definitions, if this section is retained, data principals should have the option to opt out of processing for public purposes.

  Further, '*prevention…* of any unlawful activity' is absolutely unacceptable as a reasonable ground. Technologies promising prevention of crime are ridden with problems of amplification of bias and unfair targeting. Preventive technologies are a

[1] Vinod, 2018. India's Internet shutdown rules are encouraging online censorship. *Scroll.* July 2018. https://scroll.in/article/885573/indias-internet-shutdown-rules-are-encouraging-online-censorship

classic case where firms dealing in them profit from the uptake, while the risks are socialised.

Processing of publicly available personal data is also another dangerous ground. Specifying this as a ground for which the Authority can outline reasonable purposes?, while there has been recent public uproar against social media surveillance hubs is sufficient indication of the disregard for what is considered 'reasonable' in the country.

The Authority also has the discretion to make notice requirements under Section 8 inapplicable. This is harmful, and should be omitted.

Chapter IV: Grounds for processing of sensitive personal data

- The requirement under Section 18 for explicit consent placing a higher standard of 'informed', 'clear' and 'specific' undermines consent in previous chapter. Apart from being confusing for implementation, the effect of Section 18 is that the criteria of 'informed', 'clear' and 'specific' under Section 12 are compromised. The higher standards of consent should apply to both personal and sensitive personal data equally. The difference in the extent of harm accrued if personal and sensitive personal data are breached can be accounted for in the penalties, and does not have to be accounted for in the quality of consent.

- Once again, the grounds for processing for certain functions of the State of sensitive personal data are extremely broad and leave too much room for the State. Under Section 19, 'strictly necessary' goes undefined, leaving it highly unclear what would be considered so.

- Like in the previous chapter, 'breakdown of public order' in Section 21, which allows for processing of certain categories of sensitive personal data for prompt action, tends to be generously interpreted in Section 21.

Chapter V: Personal and sensitive personal data of children

- Consent of adolescents should be distinguished from minors who are younger than sixteen years, to acknowledge the significant agency of young adults, whose interests, moreover, are not always aligned with their parents'.

Chapter VI Data principal rights

- This chapter institutes rights like the right to data portability under Section 26, which are very much welcome. However a number of standard-issue rights that empower data principals in the age of large scale data processing are missing.[2]

- A right to erasure should be included in addition to the right to data portability. Providing the latter in the absence of the former only allows data principals to exercise choice and creates a competitive ecosystem, but does not allow for control of where their data continues to be. The data storage limitation in Section 10 requires that data be deleted once the purpose of processing is complete, but in the absence of this being enshrined as a right, its value is very much diminished, as data principals lack tools to enforce it.

  The right to be forgotten under Section 27 only provides a right to limited disclosure. This is insufficient, as it does not let data principals exercise their autonomy. However, a right to erasure should be balanced with a right to freedom of speech and expression, as has been attempted for the current, limited right to limit disclosure, so that information about, say, public officials in the public domain or that is in the public interest is not erased.

- A right to object to profiling, especially when it can affect legal rights of persons should be included, and crucially, be applicable to government agencies as well. It is concerning that there is explicit provision created for the Authority to make a certain kind of profiling possible, by allowing the Authority to specify credit scoring as a reasonable ground for processing. While traditional credit scoring comes with its own set of biases, algorithmic credit scoring takes this flawed and discredited method and multiplies the harms that credit scoring systems produce. It should be great cause for worry that allowing for conclusions to be drawn from datasets which have nothing to do with financial transactions is a selling point of such systems. Existing companies that do credit scoring draw from data on social media profiles, about what games users play etc. Pushing access to banking and credit in a large way, on the one hand, and subjecting data principals to unfettered profiling on the basis of their data, on the other, is exploitative. Horrors of such scoring have been widely documented in other parts of the world.[3]

---

[2] Ranganathan, 2018. India's data protection draft ignores key next-generation rights. *Asia Times*. August 2018. http://www.atimes.com/indias-data-protection-draft-ignores-key-next-generation-rights/

[3] O'Dwyer, 2018. Algorithms are making the same mistakes assessing credit scores that humans did a century ago. *QZ*. May 2018. https://qz.com/1276781/algorithms-are-making-the-same-mistakes-assessing-credit-scores-that-humans-did-a-century-ago/

- Further, a true commitment to the collective good can be shown only by recognising that the draft Bill should apply to automated processing (including profiling) of not just personal data, but also non-personal data which leads to conclusions being drawn about groups. Without this, the many paragraphs dedicated in the report to the insufficiency of individual rights to empower citizens would be empty rhetoric. In the GDPR, this is recognised in Articles 4(4) and 22, although the extent to which it provides protection has been criticised and can do with further improvement as well.[4]

- A right to explanation should be part of the bundle of rights. At the moment, algorithmic legibility is being implemented by various jurisdictions. The GDPR enshrines a right to explanation. The lawmaking body of the city of New York passed a law requiring algorithmic accountability.[5] Making opaque decision making systems subject to scrutiny is one of the most important things that data protection legislations should do to ensure citizens have knowledge of and recourse to algorithmic decision making that can affect their rights.

- The right to confirmation and access under Section 24 should be strengthened. As it currently stands, data principals will only receive 'a brief summary' of processing activities undertaken by the data fiduciaries. This is not sufficient and should be expanded to require a copy of data held by the data fiduciary to be made available to the data principal.

Chapter VII Transparency and accountability measures

- The requirement for privacy by design under Section 29 is not meaningful. The phrase denotes well-developed principles that put the privacy of individuals at the heart of technology design.[6] Of the seven principles that are central to the concept, several are not reflected in the draft Bill: visibility, transparency, data minimisation. Exempting the State from the requirement of privacy-by-design further diminishes the true value of this provision.

- Data breach notifications under Section 32 should be amended.

    - This requirement should apply to data breaches by State actors

---

[4] Data is power: Profiling and automated decision making in GDPR. *Privacy International*. 2017. https://privacyinternational.org/sites/default/files/2018-04/Data%20Is%20Power-Profiling%20and%20Automated%20Decision-Making%20in%20GDPR.pdf

[5] Powles, 2017. New York City's Bold Flawed Attempt to Make Algorithms Accountable, *Newyorker*. December 2017. https://www.newyorker.com/tech/annals-of-technology/new-york-citys-bold-flawed-attempt-to-make-algorithms-accountable

[6] Cavoukian. Privacy by Design The 7 Foundational Principles. https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf

- The data fiduciary should not be left unguided to make a determination about the likelihood of harm to the data principal.
- The data fiduciary should be allowed to notify users directly without having to go through the Authority and should be held liable for harm caused by late or omission of notification.

- Data Protection Impact Assessments under Section 33 should take into consideration the strategic and cumulative impacts of proposals, similar to the requirements under environmental rights law and policy (for a more detailed submission on the point, please see the joint statement 'Solving for data justice: a response to the draft personal data protection bill').[7]

Chapter VIII Transfer of personal data outside India

- This Chapter brings home many of the fundamental conceptual faults of the draft Bill. The many justifications in the report for blanket data localisation requirements are not fully substantiated, and the requirements positively increase the vulnerability of data principals and decrease their autonomy and choice.

  One of the justifications in support of data localisation requirements for personal data is that it would increase the safety of such data. Given the conservative safeguards in the draft Bill, this is untrue - if anything, it increases the chances of data principals' data coming under overly broad government surveillance. Assuming the premise of enhanced safety is true, if data fiduciaries are free to have copies of personal data outside the territorial limits as long as a copy is stored in India, it defeats the said claims of enhanced safety. Such a move would also not allow smaller entities to provide services to persons based in India, impeding choice of data principals.

- By missing a chance to put into place accountability measures that allow for the government to access personal data of data principals in narrow circumstances where necessity and proportionality have been established, enforcement in fact suffers. Take, for example, the most pertinent negotiations at the moment with the United States, home to most of the tech giants that have a dominant presence in India with the Clarifying Lawful Overseas Use of Data Act (CLOUD Act). The act requires clarity of procedure amongst other things to be present in order to create a smooth channel for requests for personal data for law enforcement purposes.

- Where absolutely required for clear and specific reasons, localisation requirements can be imposed on specific sectors, like data processed for the purposes of defense etc., but a

[7] Solving for data justice: a response to the draft personal data protection bill. October 2018. https://drive.google.com/open?id=1awpQSxfqc7I4mZMYwNnnCFUYsN-h15yR

blanket requirement should not be imposed, as it ultimately hurts user choice and makes users vulnerable to greater surveillance.

- That such a blanket data localisation requirement imposes a very heavy burden on power generation in the country, and has not at all been factored into the analysis of whether such requirements are desirable. It should be considered.

- The term 'critical personal data' under Section 40 in any case has not been defined under the draft Bill and its purpose here is not clear.

CHAPTER IX Exemptions

- The exemption for 'Security of the State' under Section 42 is extremely wide. Proportionality to interests being achieved, is an acceptable standard as such if it is in addition to necessity, provided the processing of data is carried out in pursuance of a law and in accordance with the procedure established by law. However, in the absence of laws legitimising surveillance programs and absolute opacity when it comes to personal data processing by law enforcement agencies, any accountability is hard to come by. There should be judicial oversight and prior approval by courts of data processing for all exemptions for the 'Security of the State'.

- Exemption for 'prevention, detection, investigation of contraventions of law' is extremely dangerous. Particularly, a blanket exemption for *prevention* of contraventions of law is an attack on due process. Systems that come with the promise of prevention have been known to disproportionately place already marginalised persons under suspicion.[8] In light of this, creating blanket exemptions, without safeguards like transparency, will lead to an exacerbation of existing inequalities.

CHAPTER X Data Protection Authority of India

- The draft Bill does not go far enough to ensure the independence of the Data Protection Authority. Given that the bill vests numerous functions in the Authority - from research, advisory roles, rulemaking, monitoring, inquiry, and building public awareness to adjudication powers - the Authority should be independent.
    - The composition and appointment of the Authority under Section 50 is entirely up to the Central government. This is a serious compromise to the Authority's independence.
    - The composition of the Authority under Section 50 should include a requirement for representation of minority groups.

[8] Angwin, Larson, Mattu, Kirchner, 2016. Machine Bias. *ProPublica*. May 2016. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

- Similarly, under Section 68 of the draft Bill, the appointment of the Adjudication Wing is entirely up to the Central Government. This, too, is a serious compromise on the adjudicatory functions of the Authority.

We support the proposal for the Authority to be governed by a managing board.[9] We add that such a body should have representation of data principals, including specific representation of minorities, and that clear terms of reference specified under the draft Bill itself.

- Any further rulemaking by the Authority will benefit immensely from requiring an open and transparent process of consultations. This also allows for inputs about innovations in processing as well as in privacy enhancing technologies that the Authority might have missed, as well as providing all those affected by new rules the opportunity to help shape them. The quality and the extent of engagement that TRAI consultations have seen is a testament to this, and the format of the TRAI consultations - with Consultation Papers, comment rounds, the opportunity for counter comments, public availability of all inputs, and Open Houses enabling direct dialogue - should be prescribed for consultations by the Data Protection Authority in the Bill itself as well.

CHAPTER XII Appellate Tribunal

- The establishment of the Appellate tribunal under Section 79 is also up to the Central government, with no directions in the draft Bill about the selection process and eligibility of members. This should be clarified to include more specific criteria.

- A collective of data principals should be able to approach the Authority if they have been harmed in a similar way. This removes the burden of each person to have to individually approach the Data Protection Authority. Given the wide gaps in technological literacy in India, such a provision would be most useful. Under the GDPR, such a provision to authorise an entity to lodge a complaint on data subjects' behalf has been made under Article 80(1) in the name of *a representative joint action*. Further, *limited class action* under Article 80(2) allows for authorised entities act on behalf of data subjects without having obtained a mandate from such data subjects in case of a violation of the rights of a data subject under the Regulation, if the Member State has made this possible. India should contemplate introducing similar provisions in the Bill.

- Under Section 87, an appeal will only lie with the Supreme Court of India. High Courts should be able to hear appeals from the Appellate Tribunal before the Supreme Court is approached.

---

[9] Chugh, Raghavan, Kumar, Pani, 2018. Effective Enforcement of a Data Protection Regime. *Dvara Research Working Paper Series*. July 2018. https://www.dvara.com/blog/wp-content/uploads/2018/07/Effective-Enforcement-of-a-Data-Protection-Regime.pdf

CHAPTER XIII Offences

- Re-identification under Section 92 should have an exemption for security research. In the absence of this, research that ultimately strengthens the privacy of individuals and the security of systems suffers. Even then, the challenge of detection of instances of re-identification remains, and solutions should be explored.[10]

CHAPTER XV Miscellaneous

- This Chapter gives wide room for discretion to the Central Government - such as, for example, in Section 98 'Power of Central Government to issue directions in certain circumstances', Section 106 'Bar on processing certain forms of biometric data', Section 104 'Power to exempt certain data processors', and Section 107 'Power ro make rules'. This makes the Authority amenable to the government in power and compromises its independence.

- As noted before, the non-application of the draft Bill to non-personal data should be reconsidered, as conclusive anonymisation is not possible, and harm can accrue from certain kinds of processing of de-identified data sets also.

- The substitution of Section 8(1)(j) of the Right to Information Act, 2005 by Section 112 and the Second Schedule undermines the RTI Act. As at least one member of the Central Information Commission notes, the substitution has loose language that allows for information which 'relates' to personal data which is 'likely' to cause harm, after ascertaining that such harm outweighs the public interest, to be grounds for withholding of data. We support the joint statement by RTI and privacy activists on amendments proposed to RTI by Srikrishna Committee.[11]

[10] Olejnik, 2017. Reidentification ban is not a solution. August 2017. https://blog.lukaszolejnik.com/reidentification-ban-is-not-a-solution/

[11] Various activists and campaigns, 2018. Joint statement by RTI and privacy activists on amendments proposed to RTI by Srikrishna Committee. *Saveourprivacy.in*. September 2018. https://saveourprivacy.in/blog/joint-statement-by-rti-and-privacy-activists-on-amendments-proposed-to-rti-by-srikrishna-committee