Our initial comments on the Personal Data Protection Bill, 2019

In this blog post, we share our initial comments on the Personal Data Protection Bill 2019 (the Bill) that was introduced in the Lok Sabha in December 2019. Our preliminary research underscores seven key concerns that must be addressed to strengthen the proposed Bill and safeguard individuals' interests in the digital economy. These seven concerns are summarised below. A detailed 20-page document setting out research and reasoning to support these concerns, together with solutions to overcome them is available here. We welcome your feedback, challenge and comments on these initial comments.

1. User protections must be strengthened for the Bill to genuinely guarantee data privacy for Indians: We identify 7 consumer protection concerns that could weaken the citizens' right to privacy. Some are new concerns emerging in this draft of the Bill and some continue to prevail from the previous draft of the Personal Data Protection Bill released in 2018.

1.1 The Bill should not remove obligations to give notice to users where their personal data is processed without consent. The Bill dispenses with the data fiduciary's obligation to provide notice to data principals while processing personal data without their consent. Although non-consensual grounds of processing have always existed in the Bill, previously notice was required to be provided to data principals of such use in most of these circumstances except grave emergencies. The provisions in the current Bill are wider, increasing opacity for users when there is non-consensual processing of personal data. The Bill should still require notice in these circumstances.

1.2 The Bill should not raise high barriers for the data principals to withdraw their consent. The Bill makes the data principal liable for all legal consequences of withdrawing consent to process personal data unless they have a "valid reason". It is unclear why individuals should bear the threat of **all** legal consequences for withdrawal. This could disincentivise data principals from withdrawing consent. The Bill should not disincentivise data principals from withdrawing consent. Instead, withdrawal should simply result in termination of contract and discontinuation of related services.

1.3 The Bill should widen the suite of rights available to users' rights, to meaningfully empower them. The Bill contains a very limited set of rights for data principals. The absence of a full suite of user rights could result in the scales being tipped against users who may seek to achieve more autonomy and control over their data. Additional rights that can be included to level the field between data fiduciaries and data principals include: (i) right to clear, plain and understandable notice for data collection (ii) right to be asked for consent prior to data collection (iii) right to adequate data security (iv) rights to privacy by design (including privacy by default) (v) right to breach notification (vi) right relating to automated decision-making (vii) right to informational privacy (viii)

right against harm.

1.4 Data principals should not be charged fees (or be charged nominally) for exercising their rights. Data principals can be asked to pay a fee for exercising some of the rights in the Bill for e.g. the right to obtain a summary of the processing activity undertaken on their data, the right to data portability. We worry that charging a fee can raise barriers to exercise rights for low-income Indians who are becoming more digitally active but whose incomes remain low.

1.5 The Bill should not restrict users' right to seek remedies. Provisions in the Bill could limit individuals' rights to directly seek remedies in courts (where an offence is committed against them) or the Adjudicating Authority of the DPA (to initiate civil inquiries). The Bill states that a court or an Adjudicating Authority can only act upon a complaint filed by the DPA. Similar provisions restricting citizens' abilities to approach courts were held to be violative of rights by the Supreme Court when adjudging the constitutionality of the Aadhaar Act. Accordingly, these provisions (s. 83 and the proviso 63(1)) should be removed or amended.

1.6 The Bill should not make the notification of personal data breaches contingent on the breached entities' determination of "harm". The Bill requires data fiduciaries to issue a breach notification to the DPA only when they are satisfied that the breach is likely to cause harm. The DPA then determines if a breach notification should be conveyed to a data principal. Given that the concept of harm is not clear in the Bill (see point 5 below) it should not be the basis for deciding if breach notifications need to be issued. In addition, it requires that the breached entity itself that must make this determination. This could create the wrong incentives for companies suffering breaches, who now have to make a subjective decision of **whether** to report the breach. The process also creates a bottleneck at the DPA, which may delay notification of a breach to data principals. Instead, all data breaches should be reported to the DPA and data fiduciaries should have the freedom to reach out to data principals where direct actions are required following a breach.

1.7 The Bill should not weaken obligations for data fiduciaries to incorporate Privacy by Design, as this will reduce incentives to implement them. The Bill requires data fiduciaries to merely *create* privacy-by-design (PbD) policies that comply with its provisions. This obligation is weaker than that in the previous Bill which required data fiduciaries to *implement* PbD policies that would ensure compliance with its provisions.

2. The Data Protection Authority (DPA) needs to be strengthened for the new regime to be effective: The design, powers and functions of the DPA have been considerably weakened in the Bill compared to the previous Bill.

2.1 The design and composition of the DPA should be changed to maintain its independence as a regulator. The composition and design

of the Selection Committee and the Management Board are important ingredients required to create an independent, accountable and impartial regulator. Unfortunately, changes in the Bill risk compromising the quality of the future institution. No independent Members from technical and legal backgrounds are required to be part of the Board. The Selection Committee curated to appoint the Chairperson and Members of the DPA now comprises *only* Central Government officials (as opposed to the Chief Justice and an independent expert, as was previously the case).

2.2 Some substantive powers of the DPA that have been removed should be reinstated. Certain powers of the DPA have been removed or re-allocated to Central Government (compared to the previous Bill). First, the power to notify categories of sensitive personal data has been shifted to the Central Government. It is advisable for the DPA to retain this power since it is closer to the market than the Central Government with a day-to-day understanding of data practices that will enable it to make such a decision in consultation with its regulatory peers. Second, the power to notify significant data fiduciaries is not exclusively with the DPA in the Bill. The Central Government has the power to notify *social media intermediaries* as significant data fiduciaries. The power to notify significant data fiduciaries should be retained with the DPA (though it can consult with Central Government) for consistency in the delegation of powers. Third, the DPA is no longer required to publish results of inspections and other comments in the public interest. This obligation should be retained to ensure transparency in regulation, which has been proved to benefit the regulator and strengthen the regulatory regime.

3. Immense powers and exemptions for the State will limit the effectiveness of the new regime: Section 35 of the Bill empowers the Central Government to pass orders to exempt itself or any of its agencies from any or all provisions of the proposed data protection regime. This provision is a dramatic shift from the exemption for the State provided in the earlier draft of the Bill (under the 2018 draft Bill's section 42 (*Security of the State*)). It affords wide powers to the Central Government abrogate the fundamental right to privacy through executive order, without clear guidance and safeguards to fetter and guide the Central Government's exercise of power.

Other approaches such as inclusion of judicial oversight mechanisms in the section, or specifically setting out clearer conditions for the exercise of a power or the use of are better alternatives to ensure legitimacy and proportionality of this provision, and ensure it is not adjudged to be arbitrary. For instance, section 42 of the previous version of the Bill required such restrictions to be by "*procedure established by such law, made by Parliament and is necessary for, and proportionate to, such interests being achieved*". If not, in its current form the wide powers delegated through section 35 without clear guidelines for its use of other safeguards could open the provision up to the constitutional challenge.

4. The Bill should strengthen consumer protections within the proposed sandbox participants, and clarify its objectives: The Bill envis-

ages a sandbox "*for innovation in artificial intelligence, machine-learning or any other emerging technology in public interest*". However, we have serious concerns on the user protection afforded provisions in this provision. A data fiduciary that is accepted into the sandbox could be bound only by modified and diluted forms of user protection obligations in Chapter II of the Bill. Sandboxes perform experimental operations using personal data exposing users to new risks, and its effects may not be immediately understood. The Bill should clearly set out and strengthen the user protections for individuals that are common in sandbox frameworks around the world and in India (in the RBI's sandbox). Further, the objectives of the sandbox are unclear which could result in overlaps with other sandbox efforts (such as the RBI Sandbox).

5. "Harm" should not be a condition on which rights and obligations depend in the Bill: The Bill makes harm a precondition for twenty-three provisions in the Bill relating to user protection, fulfilment of provider obligations and enforcement by the DPA. This is worrying because the definition of harm in the Bill is unclear, resulting in it becoming a subjective assessment by entities, severely weakening all provisions that are predicated on the occurrence of "harm". Rights and obligations in the Bill should be fulfilled irrespective of the occurrence of harm.

6. The Bill should not include provisions relating to the sharing of Non-Personal Data: The Bill includes three new provisions relating to use of anonymised and non-personal data by the Central Government. These provisions are not related to the objectives of the Bill (i.e. personal data protection) and should not be included in the Bill. Policy on non-personal data should be dealt with separately, and by the separate Committee set up by the Government in September 2019 to study various issues relating to non-personal data.

7. The Bill should contain transitional provisions to create certainty about its implementation: The previous Bill provided transitional provisions that clearly laid down the timelines within which its provisions had to take effect, including the establishment of the DPA. Clear timelines help create political will and industry preparedness to implement the data protection regime. There are no comparable provisions in the present Bill, which can severely impede its implementation and data fiduciary compliance. The absence of a timeline to give effect to the regulatory regime for personal data processing can ultimately set back the constitutional guarantee of the fundamental right to privacy.

The detailed document containing these initial comments is accessible here. We welcome your comments and suggestions to engage further on any of these issues.