#SAVEOURPRIVACY

ADVOCATING FOR A STRONG, EFFECTIVE LAW THAT DOES NOT TREAT YOUR PERSONAL DATA LIKE OIL

Participate in the Personal Data Protection Bill, 2018 Consultation

Last year the Government formed a committee to draft a bill on data protection and privacy headed by retired Supreme Court Justice, B.N. Srikrishna. This committee has published a draft bill for consultation for which comments can be sent by September 30, 2018. [participate by clicking here]

The contents of the bill have been heavily criticised for its content and framing. [link] To help the general public, digital rights and civil society organisations participate in this process we have prepared this public guide.

This guide looks at each chapter of the draft Personal Data Protection Bill, 2018 and provides objective guidance. As with all our materials we encourage wide use, copying, remixing and adaptation with all materials under the CC-BY license.

Build your response with graded recommendations of lawyers and policy experts

Support

Lets make it better! We signify in principle support for the underlying ideas which are expressed by the provisions of the bill which may require further consultation and drafting inputs.

Improve

Hold on! Though the underlying idea is supported by us, the existing framing, structure and phrasing is either problematic or undermines user rights.

Reject

Oh no! We cite immense caution on not only the expression but the underlying idea itself. This may require a change of approach, or curing a major omission.

A 15 page guide to participate

The Personal Data Protection Bill, 2018 has 15 chapters and 112 sections. In this guide we will give top points on each one, with recommendations for you to support, improve and reject them.

This document intended as a public guide, and though it is lengthy, we hope it helps draw attention to the finer details. We encourage participation in the public consultation that is open till Sept. 30 by clicking here

The Preamble precedes the 15 chapters of the Personal Data Protection Bill, 2018. In this section we highlight how the framing indicates legislative priorities that are against the individual rights which should be at the core of such a law. In addition to this we cite the worrying omissions such as those on surveillance reform and an absence of reform of the Aadhaar, biometric scheme which have resulted in large data harms for people in India. We are also concerned with the absence of reference to the core principles of privacy protection that emerge from human rights instruments. Look up our 7 principles.

Support

- Enactment of a privacy and a data protection law ("*Whereas the right to privacy is a fundamental right and it is necessary to protect personal data as an essential facet of informational privacy*").
- The need for institutional remedy through the creation of a strong, effective and independent body to enforce privacy and data protections ("*to create a framework for implementing organisational and technical measures in processing personal data*").

Improve

- Recognition of individual autonomy as a principle in this statute. The text,"*to protect the autonomy of individuals in relation with their personal data*" must be improved to read as, "*inalienable fundamental right of all natural persons indispensable to the preservation of human dignity, personal autonomy and the exercise of constitutional liberties*".
- The objectives of the promotion digital economy and innovation are extraneous to privacy protections and should be dropped (*"and ensuring empowerment, progress and innovation;"*).

Reject

- Absence of clarity in the preamble on the principles of a, " *a collective culture that fosters a free and fair digital economy*". A "*collective culture*" is a value only insofar as it provides a context in which the individual can exercise her freedoms - but the basic unit remains the individual.
- Absence of provisions to govern, reform, and oversee surveillance in India. The draft bill must at the outset indicate that it applies to investigatory powers and surveillance actions that allow government to intrude upon individuals right to privacy in relation to communications.
- Absence of any mention of reform of Aadhaar or any other government identification program which are a major concern

Chapter 1
Preliminary

Support

- The jurisdictional scope under Section 2 is wide and pervasive. It would offer a strong basis for the application of the law on data controllers in favour of individuals.
- A key basis to our recommendation is the application of the law to the, "state" which would include most government entities and organisations.
- We support the bill in orienting the jurisdiction of the law on the basis of the users and their rights, rather than strict territorial bounds.
- The application of the protections of such a law applying only to natural persons as found in the definitions of, "data principal" and "Personal data".

Improve

- We are concerned with the absence of any definition for "collection" which is necessary given the wide data gathering exercises carried out directly and indirectly by data controllers.
- The differentiation between a data fiduciary and a data processor, needs to be explained better which have consequent effects on what obligations are placed on the latter and the role of the Authority in their regulation.
- The definition of, "sensitive personal data" needs to acknowledge that even classes of personal data can become, "sensitive personal data" depending on their context, aggregation and analysis and should permit such flexibility.

Reject

- As per the current draft bill, chapter 14 that considers the transitory provisions of the Bill is the only chapter notified after the bill receives assent from the President of India and such notification is at the discretion of the government, without any prescribed timeline. This needs to be reworked.
- Protecting and strengthening the right to privacy of the citizens of India is an urgent and pressing need, as substantiated by the *Puttaswamy judgement* of the Supreme Court of India. This Act must necessarily be notified within 15 days of receiving assent from the Honorable President of India. Hence, Section 1(3) should stand appropriately amended.

Chapter 2
Data protection obligations

Support

- We support many of the principles in this chapter however they require considerable redrafting as indicated in the column on improvements. Without such redrafting many of the principles will remain unenforceable and spur results through adjudication which will go against the rights of data subjects.
- Adjudicatory exercises to achieve clarity on the text of legislative provisions can lead to uncertain results and also undermine the basis of data protection for individuals.

Improve

- Collection of data should be limited to such data that is strictly necessary for the specific purpose of processing, and not just mere "purpose" (Section 6)
- Processing of data for an "incidental purpose" (as provided for in Section 5) must require the provision of notice to data principals (requiring improvements to Section 8)
- Notice of processing of data by a data fiduciary must be required to ordinarily take place prior to the collection of data, rather than requiring it be done no later than the exact moment of data being collected (Section 8)
- In addition to requiring a data fiduciary to indicate in its notice to data principals that they have the right to file complaints to the Data Protection Authority, the data fiduciary should provide the contact information of the Data Protection Authority (Section 8)
- In Section 8, Data Fiduciary should include in the Notice - all the obligations as provided in the Act.
- In Section 8, where data is not collected from data principal, instead of 'reasonably practicable' time period for giving notice, a time frame should be provided - 3 months perhaps.
- Under section 10(3), the data fiduciary must required to undertake periodic review to determine whether it is necessary to retain the personal data under its control, and not just possession.

Chapter 3
Processing of personal data

Support

- The principal ground for processing of personal data is consent of an individual. Specific language that strengthens the intent of such law and also makes specific provisions for persons who lack legal capacity or are unable to give consent.

Improve

- Section 12(1) should be improved such that consent is taken prior to processing of information.
- Section 12(3) may be improved such that essential services should not be allowed to be withheld from beneficiaries for want of personal data. This section must be recast in relation to essential services in a manner which shifts away from the existing framing that the provision of personal data may be necessary for such provisions. In a welfare state, identification and provision of personal data are not a quid pro quo for basic, essential services such as rations, cooking fuel, water, shelter and sanitation.

Reject

- The lack of a specific provision regarding the denial of essential services if the data fiduciary is a public authority. (Sections 12, 13)
- The idea of inferred consent currently allowed by Section 12.
- Providing loopholes to government agencies that allow them to collect data without taking consent from users. For instance Section 13(1) is unclear on what it covers, Section 13(2) provides that personal data may be collected and processed without consent by the state. That identification and provision of personal data must not be a *quid pro quo* for basic, essential services. Such benefits in most cases constitute rights of an individual, and must not be grounds for collection/processing of personal information by the state. Provision of such benefits constitute the duty of a welfare state and the individual should not be obligated to surrender their privacy for availing these services.
- Any exception to consent needs to be narrowly tailored. The carveout under 14(a) is broad and either should list existing laws and also indicate any future legislation should make a specific reference to the existing statute.
- Exceptions to employers from requiring consent from their employees when collecting their data. Section 16 should be deleted. Rather than correcting the power imbalance in a employee-employer relationship (which would normally undermine in consent based data gathering) it makes it worse, by dispensing with consent by itself of employees. An employment relationship does not lead to the cessation of fundamental rights of the employee.
- Under section 17, the Authority is provided over-broad powers of determining "reasonable purposes" as grounds for processing of personal data. Consent of the data principal is not required to be taken where the purpose of processing falls within such reasonable purposes. Provision of such wide powers to the Authority is unnecessary, and may lead to unjustified, opaque and potentially illegal processing of information, which go against the right to privacy of an individual. This section and the accompanying powers must be deleted. We, further express our objection to the inclusion of purposes such as "credit scoring" within the ambit of reasonable purposes.

Chapter 4
Processing of sensitive personal data

Support

- We support the principal ground for processing of sensitive personal data which is the explicit consent of an individual. Specific language that strengthens the intent of such law and also makes specific provisions for persons who lack legal capacity or are unable to give consent.

Reject

- The provisions of this chapter closely mirror Chapter 2 and hence we repeat our recommendations for Section 13 for Section 19; Section 14 for Section 20.
- Broad discretion has been vested in the Data Protection Authority to specify "further grounds" under which sensitive personal data may be processed which would tremendously weaken the principal requirement of obtaining consent. We urge the deletion of the following language, "may also specify any further grounds on which such specified categories of personal data may be processed." (Section 22 (1) Provision of such wide powers to the Authority is unnecessary, and may lead to unjustified, opaque and potentially illegal processing of information, which go against the right to privacy of an individual. This also goes beyond the scope of Delegated Legislation, which cannot permit addition of new substantive provisions to the Parent Act, without amending the Act.This section and the accompanying powers must be deleted.
- We further restate our suggestion for the definition of, "sensitive personal information" going beyond classes to forms of personal information which may become sensitive due to conextuality as recommended in Chapter 1.

Chapter 5
Personal and Sensitive Personal Data for Children

Support

- The clear acknowledgment that children constitute a vulnerable segment of the public, and that their interests, with respect to data collection and processing, need special focus.
- The "best interests of the child" as one of the guiding principles of the chapter.

Improve

- While the Indian Contract Act does indeed fix eighteen as the age of majority, there is no reason why the Bill - as a special legislation - cannot fix a different age, especially given the large number of online transactions persons under the age of eighteen enter into. More thought needs to be given to whether the Bill should fix a different age.

Reject

- The absence of a requirement that data fiduciaries explain to the minor, in simple and straightforward language, of the need for care in handling data (before the stage of parental consent).
- The absence of a right to opt-out upon attaining majority.

Chapter 6
Data Principal Rights

Support

- The existence of a right to data portability, including requiring it to allow such data in structured, machine readable formats [Section 26(1)]. This helps secure the interests of data principal and can help spur innovation in protecting privacy across the tech sector and industry more broadly.

Improve

- The right of a data principal to be able to access her personal data processed by a data fiduciary. A data principal must be allowed to access a full copy of her personal data processed by the data fiduciary, and not be limited only to a brief summary (Section 24). The access right must also explicitly include full disclosure of all processing, including automated decision-making, providing for a sub-provision on a right to explanation ("on a right to explanation in clear and legible language, that is understandable to the data principal."). The data fiduciary should also be mandated to provide a clear explanation to the data principal of the additional rights available to her under the Act.

- The right to correction (Section 25) is currently unclear and not strong enough for protecting the interests of data principals. The prefatory language of "where necessary, having regard to the purposes for which the personal data is being processed" should be omitted. An express and limited ground for rejection of a request for correction by the data fiduciary should instead be added, for when it proves impossible or if it involves disproportionate effort.

- The exceptions on the applicability of a right to data portability to personal data processed [Section 26(2)]. There must not be any blanket exception to the right to data portability applying to personal data processed under the "functions of the State ground". The burden to demonstrate that the portability would reveal a trade secret or would be technically infeasible must be on the data fiduciary.

- While, under section 12 and section 8, provisions have been provided wherein the data fiduciary is required to provide notice to the data principal of their right to withdraw consent, and the procedure for such withdrawal. However, no specific right to withdrawal has been provided to the user. The inclusion of an explicit right in this regard under this specific chapter of the Act is essential for the user to be able to enforce their right to withdraw from a particular service.

- Section 27 of the Bill entitles users with the right to restrict the disclosure of personal data in case they leave the service or application. However, this right has been mentioned as the right to be forgotten in the Draft Bill. The terms should not be confused. The "right to be forgotten" or the "right to de-list" entitles users with the right to request search engines to de-list web addresses from results when a search is done using their name.

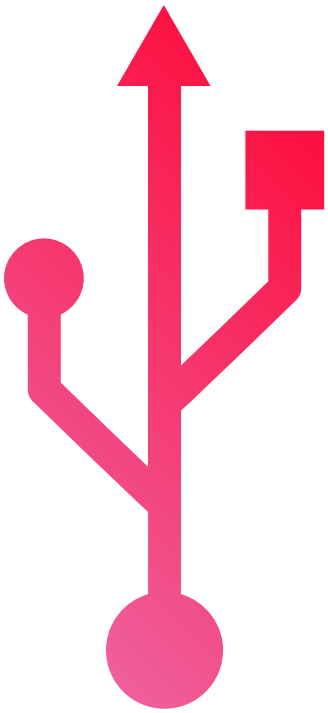
- In order to exercise certain rights, the data principal needs to provide "a reasonable processing fee" to the data fiduciary (Section 28). These rights are fundamental to a user, and user should not be charged for their exercise. If there are inordinate costs, the data fiduciary may be allowed to seek compensation subject to regulatory oversight or cost caps to be set by the Authority.

Continued..

Chapter 6
Data Principal Rights

Reject

- The absence of a right to object. Data principals must be provided an explicit right, in line with comparative standards in data protection, to be able to object and say no to processing of their personal data when they have not given consent or signed an explicit contract. This right should also apply to automated decision-making.
- The absence of a right against automated decision making. A subsequent protection is the right for the data subject to intervene.
- While under section 10, retention limitations have been imposed on the data fiduciary, and under section 27, a right to prevent disclosure of information has been provided after one leaves a service or application, no direct right to erasure has been provided. This right is essential to ensure that data trails are effectively deleted, due to the large number of services and application present in the world right now.
- The right to be forgotten under Section 27 refers to the relevance and impact of the right to be forgotten on the right to information. This is a matter of extreme concern as any interactions between the right to privacy and data protection with the right to information need to be determined as per the guidance and process as provided by the Right to Information Act. We would further urge and caution against any dilution of the Right to Information laws. In the instance any request is made with respect to an analysis or concern of, or related to the Right to Information Act, the authorities under the data protection law should return a finding indicating a lack of jurisdiction.
- The exercise of the rights granted under the Draft Bill may be limited by the data fiduciary, wherein a data fiduciary may refuse the data principal, in cases where the exercise of the right would harm the right of any other data principal (Section 28). This criteria for rejection is over-broad and liable to misuse. Limitations to rights of users should be narrow and specific with clear avenues for redress.



Chapter 7
Transparency and Accountability Measures

Support

- Section 29 introduces the principle of privacy by design, which provides the data fiduciary with the responsibility to implement policies and measures for privacy by design.
- Section 31 puts the obligation on the data fiduciary and the data processor for implementation of appropriate security safeguards.
- Section 33 puts the responsibility on the data fiduciaries for conducting data protection impact assessment, especially, whenever new technologies are introduced, or they use sensitive data or carry out large-scale profiling.
- Section 30 holds the data fiduciary responsible to notify the data principal of important operations in personal data processing.
- Section 34 & Section 35 of the Draft Bill specifies the provisions and makes it mandatory for data fiduciaries to maintain records and be subjected to annual data

Improve

- Section 30 information on transparency processes followed by a Data Fiduciary should be clearly indicated to be made publicly available. The practices of data fiduciaries in dealing with government (especially law enforcement) need to be publicly revealed.
- Under the transparency requirements provided in section 31, data fiduciaries must also be required to disclose findings from the data impact assessments as well as data audits.
- Under section 38, certain transparency and accountability provisions such as record keeping, data protection officer, data protection impact assessment, data audits are applicable only to "significant data fiduciaries". We believe that blanket exemptions for any data fiduciary from such requirements should be avoided. The Authority may provide differential level of compliance based on the capacities of various levels of data fiduciaries, maintaining a baseline compliance standard.

Reject

- We believe that Section 32 requires a complete redraft and in its present form must be rejected. Given that a determination on disclosure by the DPA to the Data Fiduciary for a breach notification to persons may incur time, we believe it is necessary for an independent duty on it to inform a person if personal data is affected and is likely to have an impact on a person's private life, those breaches should be notified without undue delay, and in no event later than 72 hours after the company becomes aware of it. Further, the existing criteria for disclosure to persons as determined by the DPA is set to a high threshold of gauging, "the severity of the harm" or, the requirement to, "mitigate such harm". We believe this standard is wrong and people in all instances need to be informed of data breaches when it concerns their personal data and has an impact on their personal life. Additionally, in case such information is only disclosed to the Authority - the Authority must make public the criteria for its assessment of harm to the user from a data breach and such criteria must include a human rights impact assessment.
- While the provision, under section 36, a Data Protection Officer provides an ease in enforcing provisions of this law. However, by requiring the physical presence of such officer within India, an inordinate cost of compliance has been put on web services and applications, beyond the big technology platforms. Thereby resulting in harms to people in India, without conferring any data protection benefit to individuals in India.
- Any rights and protections available to users with respect to the data fiduciary, must be equally applicable with respect to a data processor as well, under section 37.

Chapter 8
Transfer of Personal Data Outside India

Support

- Section 41 of the Draft Bill specifies provisions for cross-border transfer of non-critical personal data. These provisions are similar to the GDPR. According to the section, the cross-border transfer of personal data is permissible when the Central Government in consultation with the Authority prescribes to so. The Central Government may ask for cross-border data transfers only where it finds that the personal data shall be subject to an adequate level of protection, having regard to applicable laws and international agreements.

- Additionally, data transfers may also be made subject to *standard contractual clauses or intra-group schemes* that have been approved by the Authority. These provisions are positive and help in harmonising the Indian law with international jurisprudence, while ensuring the rights of users in India.

Improve

- Under section 41, the Authority is provided the power to approve a particular transfer or set of transfers as permissible due to a "*situation of necessity*". The use of such words brings in ambiguity and render such provisions to misuse, which may result in the rights of users being violated.

- There is no guidance provided regarding such situations of necessity. Such situations of necessity must be based on narrow, and specific standards which must be explicitly mentioned under the Act.

Reject

- The Draft Bill troublingly seeks to establish a data localisation / mirroring regime in India.

- Section 40 of the Draft Bill makes it mandatory for every data fiduciary to store one serving copy of every personal data on a server or data centre located in India. This section dilutes India's connection to the global internet and betrays a governmental interest in desiring more control over the data of Indian citizens.

- The report submitted by the expert committee enlists enforcement and access as the primary motives behind this requirement. However, data localisation is not - and should not - be a prerequisite for enforcement of data protection rules. What is more, such a requirement may facilitate third party abuses of personal data and infringe on users' right to privacy as actors would know where data is located.

- Such proposals go against the spirit and objective of a data protection and privacy legislation. Curiously, there is an exception created to this rule wherein the Central Government may notify certain categories of personal data as exempt from the requirement of local storage on the grounds of necessity or strategic interests of the State. There is however no guidance provided regarding such strategic interests or necessity.

Chapter 9
Exemptions

Support

- Exemptions provided for personal / domestic use, journalistic use, and research purposes are necessary exemptions. These may require further review and redlining to prevent unintended consequences of either broad privacy violations or fetters on the legitimate exercise of free expression and speech.
- There is support for an interpretation that mass surveillance is now illegal per se which needs further clarity. Given the acknowledgment of a three part test: (a) authorisation pursuant to a law (+ in accordance with procedure established by law), (b) demonstrated necessity; and (c) proportionality for sections 42 and 43. This means mass surveillance measures or surveillance measures that are not authorised by law, e.g. CMS (Central Monitoring System), will be in violation of the Act.

Reject

- Under this chapter, exemptions from privacy right of citizens in India, is provided for the government for reasons of "security of state" (section 42) as well as "prevention, detection, investigation and prosecution of contraventions of law" (section 43). The requirements in sections 42 and 43 endorse the current antiquated surveillance framework that exists in the country under the Telegraph Act and the Information Technology ("IT") Act. Notably, these laws do not require any prior judicial authorization to conduct surveillance, and instead rely on executive sanction by a competent authority.
- While section 30 of the Bill requires data fiduciaries to take "reasonable steps" to maintain transparency and section 35 recognises data audits, there is no direct requirement for law enforcement agencies to submit a report to Parliament about the nature and scale of their surveillance and interception activities.
- One of the biggest problems in terms of surveillance reform has been the judicial sanction to admit illegally obtained evidence, including tape-recorded conversations. This skews the incentive of law enforcement agencies to comply with the (already weak) safeguards that are recognised in the law. Evidence obtained without proper and prior judicial sanction must be disallowed.
- Data protection and surveillance reform are complementary to each other in ensuring the privacy rights of users - this Draft Bill does not provide any surveillance reforms and is thus a missed opportunity to provide effective data protection in that regard.

Chapter 10
Data Protection Authority of India

Support

- Section 49(4) allows the DPA to have regional offices, so it is not as if we only have a central DPA. However, one issue is that unlike the Consumer Act, this does not require the establishment of state and district DPAs with different pecuniary jurisdictions. Given the number of complaints that are likely going to be heard, there is a serious state capacity issue here. We urge that learnings on central and state level authorities may be established as indicated in the Indian Privacy Code, 2018.

Improve

- Independence of the appointment process from executive branch control. Currently, the appointment committee is supposed to be composed of the Cabinet Secretary, the Chief Justice of India or her representative, and a third person that is to be recommended by the CJI or her representative (Section 50). The CJI is only allowed to recommend someone based on a shortlist of 10 names that the Cabinet Secretary will prepare, undermining the independence of that appointment and potentially allowing the Union Government of the day to pack the appointment committee.
- All appointments to the positions of Chairperson or Member of the Authority must be done after public notice/advertisement for applications.
- On avoidance of conflict of interest of the Chairperson and Members of the Authority. There currently is no requirement for the members of the DPA to disclose or avoid any conflict of interest (Section 51). The restriction on post-term employment is limited when it comes to possible private sector jobs, since it only speaks of appointment with "a significant data fiduciary".

Reject

- The lack of a clear mandate for public consultation for all regulation setting by the Authority.
- The complete control and discretion of the government in appointing Adjudication Officers under section 68.
- The adjudication wing and regulation wing should not be housed within the same body because in practice then the one arm distance will not be maintained.

Chapter 11
Penalties and Remedies

Support

- We support the provisions for penalties under Sections 69 and 70. However there is an absence of considerations on how penalties and fines will be evaluated against state entities.

Chapter 12
Appellate Tribunal

Reject

- The absence of any provision on the composition of the Appellate Tribunal is a matter of extreme concern given issues of conflict of interest, proper static and capacity.

Chapter 13
Offences

Support

- We support the existence of criminal offences for contraventions of this law as specified under Sections 90 and 91.
- We support criminal liability being imposed on the head of a government institution under Section 96 as they are in charge and overall direction of the use of personal data by their departments.

Improve

- The criminal penalty for re-identification as specified under Section 92 proceeds on the lack of permission from either the data fiduciary or controller, which should rather be the person whose anonymised data is then used to re-identify them.

Chapter 14
Transitional Provisions

Improve

- The bill currently does not provide any obligations with respect to data collected / processed before the enactment of the bill. Specific opt out provisions must be provided wherein data principals must be allowed to opt out in relation to collected / processed before the enactment of this bill, and an obligation to delete / anull such data / processing must be put on the data fiduciary, if such an opt out provision is availed by the data principal.

Reject

- Under section 97(8), a long waiting period of 18 months is provided after the enactment of the bill, for the coming into effect of majority of the provisions of this bill. Such a long waiting period is unacceptable - the majority of the Act cannot come a full 18 months after its passing.
- A data protection reform in India is needed urgently, and the act must come into force much earlier. The bill provides a period of 12 months within which the law may be notified by the government. This period is too long, and the law must come into effect immediately after receiving assent from the President of India.

Chapter 15
Miscellaneous

Improve

- While we support the power to bar the processing of certain forms of biometric data through notification, the determination of such a bar should not be made by the Central Government directly as presently contemplated under Section 105 but be left to the Data Protection Authority.

Reject

- The power to issue directions by the central government to the Data Protection Authority as permitted under Section 98 provide wide discretion which would undermine it as an independent statutory authority. This becomes important given the role and extent of the processing of personal data by the state.
- The power to remove difficulties has been an instrument to recast the parliamentary function of legislation and we recommend the deletion of Section 103.
- We reject the amendments sought to be made to the Right to Information Act which should not be subject to amendments made by a Data Protection law given the pre-existing protections under it. We again cite concern on the absence of reform and amendment of the Aadhaar Act, which principally conflicts with any data protection law and standards.