Jan. 25, 2020

INTERNET FREEDOM FOUNDATION

SAVE OUR PRIVACY

A public brief and analysis on the **Personal Data Protection Bill, 2019**

IFF's briefs focuses research to support public understanding on issues of digital rights

Further analysis and guides available at : saveourprivacy.in

#SaveOurPrivacy

The #SaveOurPrivacy campaign has close to 11,000 individual and 27 organisational supporters who have pledged support to its 7 privacy principles and a model law titled as the, "Indian Privacy Code". The Indian Privacy Code has been filed twice as private members bills in Parliment.

#SaveOurPrivacy has worked since May, 2018 as a framework for civil society groups to put forward demands on data protection and surveillance reform. It has influenced and brought accountability to the drafting process of the Personal Data Protection Bill.

This brief has been authored by SaveOurPrivacy volunteers (Maansi Verma, Vrinda Bhandari, Gautam Bhatia, S. Prasanna, Raman Chima, Anushka Jain, Apurva Singh, Shreya Tiwari, Ishika Garg and Apar Gupta,) to assist legislative engagement.

#SavingTheInternet

The Internet Freedom Foundation works on issues of online censorship, advocating for privacy, safeguarding net neutrality and innovation.

It is a registered 80G non-profit funded by Indians and represents the interests of individual Indians.

We are guided by values of human freedom from the Constitution of India. Born out of the #SaveTheInternet.in campaign for Net Neutrality, IFF today supports research, advocates civic education, builds participatory campaigns, engages with regulators and approaches courts.

IFF powers the community driven #SaveOurPrivacy campaign.

For SaveOurPrivacy: www.saveourprivacy.in

For IFF: www.internetfreedom.in

6 Key facts on legislative history

1. **Present status:** The Personal Data Protection Bill, 2019 was introduced in the Lok Sabha by Union Minister of Electronics and Information Technology, Mr. Ravi Shankar Prasad, on December 11, 2019. A Joint Parliamentary Committee was formed on December 12, 2019 to review the proposed Data Protection Bill which is expected to give its report by the last week of the budget session of 2020.[1]
2. **Past efforts:** Previous versions of a Draft Privacy Bill have been coordinated through the Ministry of Personnel, Public Grievances and Pensions since 2011.[2] Drafts of this Bill dealt both with Data Protection and Surveillance Reform till 2014 - however this did not proceed further.[3] An Expert Committee on Privacy headed by Justice A.P. Shah under the erstwhile Planning Commission presented a report on October 12, 2012 which serves as an influential document on international & national privacy standards.[4]
3. **Private Member Bills:** There have been six notable efforts to introduce various models of privacy protection by honourable members of the Lok and Rajya Sabha. These are listed in a tabular form below.

House and date	Short title (click to download)	Member	Status
Lok Sabha on 04/03/2011	Intelligence Services (Powers & Regulation) Bill, 2011	Manish Tewari	Lapsed
Rajya Sabha on 05/08/2016	Right to Privacy of Personal Data Bill, 2016	Vivek Gupta	Lapsed
Lok Sabha on 10/03/2017	Right to Privacy of Personal Data Bill, 2016	O.P. Yadav	Pending
Lok Sabha on 21/07/2017	Data (Privacy and Protection) Bill, 2017	Baijayant Panda	Lapsed
Lok Sabha on 03/08/2018	Data Privacy and Protection Bill, 2017	Shashi Tharoor	Lapsed
Lok Sabha on 26/07/2019	Personal Data and Information Privacy Code Bill, 2019	D. Ravikumar	Pending

4. **Right to Privacy Judgement:** On 24th August, 2017, the Supreme Court in the matter of *Justice KS Puttaswamy vs Union of India* reaffirmed "privacy" as a fundamental right under Part III of the Constitution of India. It directed the Government to bring out a robust data protection regime.[5]
5. **Srikrishna Expert Committee:** The Expert Committee on Data Protection chaired by Justice BN Srikrishna was constituted by the Ministry for Electronics and IT on 31st July, 2017.[6] It was criticised for its flawed composition and issues of conflict of interest.[7] The Committee released its Report and proposed the Personal Data Protection Bill, 2018 on 27th July, 2018.
6. **Consultation by MIETY:** The PDP Bill, 2018 was open for comments in a consultation organised by the Ministry for Electronics and IT till October 10, 2018. However the comments, changes made to it, reasons and who made them were not made public by the Ministry. These changes were forwarded to the Union Cabinet and thereafter introduced in the Lok Sabha as the PDP Bill, 2019.[8]

---

[1] *https://prsindia.org/billtrack/personal-data-protection-bill-2019*

[2] *https://pib.gov.in/newsite/erelcontent.aspx?relid=74743*

[3] *https://cis-india.org/internet-governance/blog/report-of-group-of-experts-on-privacy-vs-leaked-2014-privacy-bill*

[4] *https://iltb.net/summary-of-the-report-on-privacy-law-by-the-group-of-experts-headed-by-justice-a-p-shah-6e5917ea9c18*

[5] *https://indiankanoon.org/doc/91938676/*

[6] *https://pib.gov.in/newsite/PrintRelease.aspx?relid=169420*

[7] *https://indianexpress.com/article/india/citizens-group-questions-data-privacy-panel-composition-aadhaar-4924220/*

[8] *https://saveourprivacy.in/blog/the-purpose-of-public-in-public-consultation-lest-we-merely-consult*

Summary of top 10 issues

Loopholes in the PDP Bill, 2019

1. **Lack of clarity on the objectives :** From the time of the Justice Srikrishna Committee, the PDP Bill has suffered a lack of clear focus on data protection. Instead it has incorrectly sought to promote private and state interests. This has resulted in confused drafting choices.

2. **Preference to private and fiscal interests over data protection:** The PDP Bill, 2019 creates large carve-outs for anonymised non-personal data, sandboxes that would undermine the privacy rights of individuals on grounds of lack of consent. There peculiar insertions not found in global data protection laws.

3. **Collection of data without consent and denial of services:** There exist broad conditions which can make the government and other entities collect data without consent and also deny essential services.

4. **Strengthen user rights:** While several user rights are present, rights such as being exempt from automated decision making are not granted to people. Further exemptions and carve-outs need to be re-examined.

5. **Social Media Entities**: The provisions with regard to social media entities using government ID's for verification is completely misplaced. It would have several harms, increase surveillance and profiling.

6. **Data localisation**: The data localisation provisions are improperly placed within the data protection law. They are broad, vague and provide tremendous discretion to the government.

7. **Surveillance reforms**: One of the most obvious deficiencies of the PDP Bill, 2019 are the large exemptions provided to Government by which it can exempt it's own departments from application of the law. Further, there is a complete absence on seizing the historic opportunity for surveillance reforms.

8. **DPA's selection, staffing and independence**: Another core deficiency in the PDP Bill, 2019 is the lack of independence of the DPA's selection body which comprises only of government officials without having any judicial, opposition or civil society membership. This becomes important given that the DPA is institutionally meant to protect individuals both against private and government entities.

9. **Miscellaneous:** Provisions on impact to the RTI Act and the need for application of the protections to only natural persons must be considered.

10. **Protection for vulnerability testers and whistleblowers:** The exemptions within the PDP Bill need to spell out clear protections for those who protect and further cyber security by vulnerability testing and reporting on breaches.

Analysis

Concern and clauses	Analysis	Recommendations
1. Lack of clarity on the objectives **Preamble**	The preamble of any law sets the tone and the tenor of a law and is crucial in understanding the intent behind the legislation. The preamble, along with the objects, is also a key factor influencing the judicial interpretation of various provisions of the law. The preamble of the PDP Bill, 2019 contains objectives on creating a collective culture which promotes a free and fair digital economy, progress and innovation, while respecting informational privacy. Such emphasis on promoting digital economy through a data protection legislation - rather than prioritising the rights of Indians - is misplaced. There seems to be a tangential focus on economisation of data as opposed to a clear and unequivocal emphasis on the individual privacy as a fundamental right. The preamble also makes no mention of safeguarding a citizen's right to privacy from the state. The history of the evolution of the right to privacy, both globally and in India (especially as happened by the Aadhaar litigation), demonstrates a recognition of the need to protect privacy against State action. A modern data protection legislation must not only embody this recognition, but go further and exhort the State to be a model data controller.	The preamble be suitably amended to state, in no uncertain terms, that protection of data and informational privacy, from private as well as state actors, is the overriding objective of the PDP Bill. Once a data protection law and its modalities are in place, suitable compliant norms can then be designed for other related concerns. The preamble must also be suitably amended to state the principle of the State needing to be a model data controller. Here, we must refer to the individual rights of natural persons in line with the Supreme Court's right to privacy judgement and the model privacy principles recommended by the A.P. Shah Expert Committee Report
2. Preference to private sector and financial interests over data protection **Clauses 2(B); 3(2); 3(3); 40; 91.**	Provisions of the PDP Bill will not apply to anonymised data (Clause 2(B)). Anonymised data is such which has gone through an irreversible process of transforming or converting data to a form in which the data principal cannot be identified as per standards of irreversibility specified by the Authority (Clause 3(2) and 3(3)). However, in consultation with the Authority, the Central Government can mandate any data fiduciary or processor to provide it with anonymised personal data or other non-personal data (defined as data other than personal data) for better targeting of services and "evidence based policy making". The Central government may also frame policies for the digital economy as long as it does not govern personal data (Clause 91). There is no clarity on what is non-personal data. The definition of anonymised data is not comprehensive and leaves out the possibility of identification of data principal by combining anonymised data with other data - which is increasingly possible today. Additionally, the Bill provides for setting up of a 'Sandbox' to privacy regulation, without even defining the term anywhere (Clause 40).	A data protection legislation must not have an enabling provision for the government to mandate sharing of non-personal and anonymised data with it, for setting up regulatory 'sandboxes' and for framing policies on digital economy, especially when the possibility of misuse of anonymised and non-personal data and threats arising from new technology have not been sufficiently addressed. Real possibilities exist of identification and subsequent targeting of individuals and communities from seemingly non-personal data. These provisions are not usually present in Data Protection Acts globally and are a deviance from the objective of the present legislative proposal. We recommend their deletion.

Concern and clauses	Analysis	Recommendations
3. Collection of data without consent and denial of services **Clauses 11; 12; 13; 14; 16.**	Clause 12 lays the grounds under which personal data may be processed by the State without consent of the data principal, including for providing services, benefits, licenses, compliance with judgment or order of the courts, to respond to medical emergencies, undertake measures during disaster or any breakdown of public order. Additionally, the exemption from consent also applies to personal data collected by employer for recruitment, verifying attendance, performance assessment etc.(Clause 13) and even to other 'reasonable purposes' (to be identified through regulation) which can range from whistle-blowing to operation of search engines (Clause 14). These exemptions are broad, vague and pose concerns on excessive delegation and undermine the right to privacy. It further requires consent on behalf of minors to be given by a guardian and a responsibility is put on data fiduciary to verify the age of data principal (Clause 16). It is provided that the provision of a good or service or enjoyment of a legal right or claim etc. shall not be denied for want of consent to process data not necessary to that purpose. However if consent given is later withdrawn, without any valid reason, the data principal will be liable for all legal consequences (Clause 11). There is no express bar on denial of essential services and it is not clear whether such legal consequences will amount to denial of essential services. This is important to note because there have been many instances where essential services like rations, medical aid have been denied to beneficiaries.	It is imperative that the Bill provide an explicit bar on denial of essential services for want of personal data or at the very least be based on the impossibility of providing the service. It must mandate for a data fiduciary to provide for and accept less intrusive alternatives to particular personal data. It is also important that any collection of data without consent is strictly for a limited purpose and the law shouldn't provide any scope for further addition to this through delegated legislation. A child should be able to rescind consent upon attaining majority; other people who may be incapable of giving consent should be covered. Regarding use of data by employer without consent reference may be made to Article 88 of European Union's General Data Protection Regulation, which provides for processing of employee's personal data in context of employment while safeguarding human dignity, legitimate interests and fundamental rights - especially with respect to transparency of processing.
4. Strengthen user rights **Clauses 18; 19; 21; 25.**	Clause 18 contains the right to correction, completion, updation and erasure of data but are limited as the data fiduciary's obligation to respond to these rights has been made conditional and it may even refuse a user request. Clause 19 contains the right to data portability but again, data fiduciary may deny on grounds of technical infeasibility or protection of a trade secret. Here, personal data is not a trade secret as it primarily concerns the fundamental rights of persons. Clause 21 provides that for complying with requests made by data principles in exercise of their rights, data fiduciary may charge a fee. These rights are fundamental to a data principal, and she should not be charged for their exercise beyond a nominal fee. Clause 25 provides that in case of a breach of data, data fiduciary shall inform the Data Protection Authority, as soon as possible, where such breach is likely to cause harm to any data principal.	Clauses 18, 19, 21 and 25 need to be reviewed in an analysis in which the individual right to privacy receives primacy and the interests of data fiduciaries are limited exceptions, if any. Specifically, Clause 25 that empowers the DPA to determine whether to keep the data principal in dark in case of a breach of their personal data requires change to make disclosure of the data breach a rule. As far as possible, any unnecessary or unreasonable restrictions should not be placed on the exercise of rights. Further rights such as the right to seek exemption from automated decision making, especially when it can lead to violation of rights require inclusion.

Concern and clauses	Analysis	Recommendations
5. Social Media 'Registration' and Data Retention **Clause 26**	A social media intermediary has been defined in the Bill and it is provided that it can be categorised as significant data fiduciary depending on number of users and impact on electoral democracy, security of state, public order etc (Clause 26). Such social media intermediaries will have to enable their users to verify their accounts "voluntarily" in such manner as may be specified, and such verified accounts may be identified with some visible mark. It will adversely affect whistleblowers, victims of sexual assaults who often resort to anonymous identities on social media websites to share their experiences. It is not clear if the means devised are suitable to address the identified purpose. It will lead to further data collection by large social media companies on the basis of Government IDs and to the contrary facilitate more targeting and surveillance. Such a provision is not found in any data protection law globally and is a deviation from established privacy norms. This provision will also increase the risk from data breaches and entrench power in the hands of large players on the internet who can afford to build and maintain such verification systems. There are concerns that intermediaries through changes in the Information Technology Act, 2000 and its rules will have to report accounts that do not verify themselves to the government, which could make them a target for political censorship and chill dissent.	The vagueness and over-breadth of Clause 26 makes its constitutionality suspect. This provision must be removed and any regulation of social media intermediaries other than data protection must be through specifically tailored laws that Parliament carefully reviews and are careful about respecting fundamental rights. Concerns on social media companies (other than personal data) need to be considered separately under legal frameworks of electoral, intermediary liability, and competition law.s
6. Local data storage **Clauses 33; 34**	While there is no requirement for localisation for "personal data", the Bill however does state that "sensitive personal data" may be transferred outside India (by asking for explicit consent from data principal and taking additional safeguards including determination of whether adequate protection will be offered), but shall continue to be stored in India. "Critical personal data" is not defined in the Bill, Further the government is empowered to define critical personal data at a later stage, which may not be transferred outside India at all except for prompt action during a health emergency or to a country, entity or international organisation to whom Central Government deems permissible to transfer (Clauses 33 and 34). This provides the government with powers to collect and process data and when the Bill additionally mandates storing and processing sensitive and critical personal data in India, it is likely to create concerns of unbridled intrusion into privacy by the state. In the EU's GDPR, there are two categories of data- personal data and special categories of data. The former is similar to the definition of personal data in the Bill. The latter includes data pertaining to race, ethnicity, political opinions, religious beliefs etc. It is important to note that data localisation requirement is absent in GDPR.	The Bill must not mandate storing or processing of data only in India. Free flow of data, with adequate safeguards to ensure that data protection rights apply to the data of Indians no matter where it may be transferred truly protects privacy in our internet age while also helping make India a valuable player in the globally networked trade regime. Critical Personal Data, if at all, must be defined in the Bill itself by Parliament. It can not be left to be defined by the executive without any guiding principles.

Concern and clauses	Analysis	Recommendations
7. Surveillance Reform **Clauses 35; 36; 37**	Clause 35 of the Bill empowers the Central Government to exempt by an order, 'any agency' of the government from all or any provisions of the data protection law if it is in the interest of the sovereignty and integrity of India, the security of the state, friendly relations, public order and to prevent incitement to the commission of an offence. The only safeguard is that the written order from the Central Government must specify the reasons for such exemptions, ignoring the requirements otherwise established in Indian and international law of meeting the test of being "necessary and proportionate". These exemptions will not just apply to data gathered by such agencies, but also with any data that is shared with such agencies by other data fiduciaries. It puts the power in the hands of the Central Government and specifically makes it the judge and adjudicator of its own cause. Clause 36 of the Bill also creates specific exemptions in certain cases, to which no safeguards will apply. Clause 37 which is supposed to empower the Central Government to exempt the processing of data of foreigners by data processors is also vaguely worded. Most intelligence agencies of India suffer from a lack of institutional oversight and there are no laws clearly defining their powers or limitations to those powers. Further, there is the lack of any serious review of telephone tapping and other communications interception powers in the Bill. This will make personal data of citizens open to mass surveillance and make the protection meaningless.	Existing exemptions are too vague and broad and must be narrowly tailored. A complete chapter on surveillance reform needs to be inserted in the present PDP Bill. Government agencies responsible for carrying out surveillance and interception as part of their law enforcement functions must be clearly identified, notified, and bound by the provisions of the Bill. A procedure must be put in place for such agencies to seek permission from a judicial authority - preferably by special benches or tribunals comprising of High Court judges. Additionally, an appropriate oversight and accountability structure should be created as part of Data Protection Authority by adding within it an an office for surveillance reform and oversight. Judicial permission that may be granted for emergency surveillance and communications interception must be required to follow the necessity and proportionality principles. To administer such judicial orders, the Data Protection Authority may determine compliance and enforcement mechanisms.
8. DPA's selection and lack of independence **Clauses 42; 62; 63; 86**	As per Clause 42, the Selection Committee for appointing members of the Authority will comprise entirely of members of the executive. The Srikrishna Committee draft bill of 2018 had prescribed a diverse selection committee with executive, judicial, and external expertise. Given that this proposed law is also safeguarding user data from the government, there is a lack of impartiality because the government itself will exclusively bring in place the governing structure. This will make it much harder for the DPA to be an independent and effective regulator. The Bill further impedes the independence of the DPA by empowering the Central Government to issue binding directions to the DPA (Clause 86). It must also be noticed that for the anticipated number of data protection grievances that people may have, there is no decentralization of the DPA to establish state level authorities. This can lead to pendency in the long term. Lack of independence of the adjudication wing is also of concern, since Adjudication Officers will be appointed by the DPA (Clause 62) and will only adjudicate enquiries initiated on complaints made by DPA (Clause 63).	The composition of the Selection Committee must comprise of a judicial authority, an executive authority and external members. The process for appointment of the DPA Chairperson and Members must be transparent with an open call for applications and proceedings of the Committee must be a matter of public record. There must be a bar on persons with vested political or business interests to be appointed to the DPA. State level DPAs must be set up by enabling State Governments to do so, in line with other state level regulators like State Information Commissions. Appointment of Adjudicating Officers should also be through a transparent process and by independent bodies designed to select judicial officers. Central government must not have any power to issue binding directions to the DPA.

Concern and clauses	Analysis	Recommendations
9. Miscellaneous **Clause 96; Schedule**	It is important to note that the Bill doesn't acknowledge a natural person as owner of their data. The Bill also doesn't deal with data collected prior to the Bill coming into force and has no transition provisions. Additionally the Bill has been given an overriding effect (Clause 96). The EU GDPR repealed the EU's pre-existing Directive 95/46/EC popularly known as the Data Protection Directive. Recital 171 of GDPR provided that processing already underway under the earlier Directive should be brought into conformity with GDPR within two years after which this Regulation enters into force. Where the processing consent is based on the Directive, it is not necessary for the data subject to give consent under GDPR again if the consent has been in line with GDPR.	The Bill must categorically acknowledge a natural person as owner of her data. The Bill must additionally provide that data collected prior to this law coming into force, if collected in a manner inconsistent to the law, must be destroyed if the consent is withdrawn. Finally, the Expert Committee Bill had sought to amend the Right to Information Act specifically, whereas the current Bill has an overriding clause, and both may ultimately lead to undermining the RTI Act by stifling transparency. The Bill must specifically state that provisions of RTI Act will have precedence over this law in case of inconsistency.
10. Protection of whistleblowers, digital security researchers, vulnerability testers **Clauses 25; 38; Schedule**	In several cases of breach of the obligations under the Act - particularly in relation to the breach of the limitation of purpose obligation, unauthorised sharing or a non-notification of a security event, the data principal is often in the dark and is not in a position to enforce her rights due to the asymmetry of information. At present Clause 25 only provides for a data fiduciary to report such breaches and lapses rather than whistleblowers. It is important therefore for the Bill to provide an institutionalised mechanism for personnel of the respective data fiduciary to safely, and freely without any fear of retaliation or retribution, report such breaches. While research is exempted from the obligations of Clause 38 there are no clear protections for skilled cyber security researchers who conduct vulnerability testing. Many such persons are put to harassment by vexatious legal claims and proceedings.	The Bill must make amendments to provide include clear provisions detailing the procedure for security researchers, vulnerability testers, data breach reporting and whistleblowers to the DPA with suitable amendments to Clause 25. This is in addition to the direct breach notifications we have recommended above. Further amendments must be made to Section 43 of the Information Technology Act, 2000 to prevent vexatious legal claims and proceedings against vulnerability testers and cyber security experts. We recommend that narrowly tailored good faith exceptions must be added by way of an amendment to the Schedule.

Contact us!

Whether you are a Member of Parliament, a technologist who works with data or an ordinary person intrigued by privacy; we encourage you to reach out to us!

We offer regular briefings and deconstruct some rather complex and nuanced policy debates into helpful guides and encourage wider pubic participation.

Just email us on policy@internetfreedom.in

INTERNET FREEDOM FOUNDATION