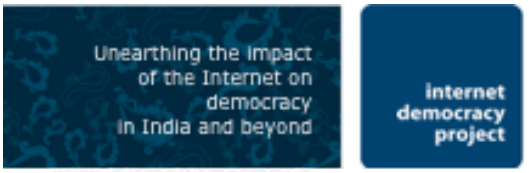

Personal Data Protection Bill 2019

Submission to the Joint Parliamentary Committee

By the Internet Democracy Project

The Internet Democracy Project (https://internetdemocracy.in/, http://genderingsurveillance.in) works towards realising feminist visions of the digital in society, by exploring and addressing power imbalances in the areas of norms, governance and infrastructure in India and beyond.

The Internet Democracy Project welcomes the consultation by the Joint Parliamentary Committee on the Personal Data Protection Bill 2019 and we would like to thank you for this opportunity to present our comments on this important Bill.

In the interest of a transparent process, we hope that all responses will be made public along with the report furnished by the Committee.

The starting point of our submission is the strong emphasis that the Bill puts on the fiduciary relationship. A fiduciary relationship is a relationship of trust, between two parties a fiduciary and a beneficiary, wherein the fiduciary is expected to concentrate only on conferring benefit to its beneficiary.[1][2] While fundamentally, there may be a power imbalance between a fiduciary and a beneficiary by virtue of knowledge, power or position, however there exist certain checks and balances to ensure that a fiduciary does not breach any of its fiduciary obligations.

This Bill intends to adopt the concept of information fiduciaries[3] by creating a fiduciary relationship among data collectors/processors (fiduciaries) and data principals (beneficiaries), and by imposing certain data protection obligations, transparency and accountability measures upon data fiduciaries. The Bill also lays down offences and punishments to prevent breach and misuse of personal data by data fiduciaries.

However, upon closer examination, it is clear that the Bill fails to do justice to the use of terminology 'fiduciary relationship'.

---

[1] It must observe a high duty of care and loyalty, must go beyond ordinary to avoid harm to its beneficiary- Birbaum v Birnbaum, 539, NE 2D, 574, 576 (N.Y 1989).

[2] Fitzgibbon, Scott T (1999). Fiduciary Relationships Are Not Contracts. *Marquette Law Review,* 82. Page 303-354. .https://lawdigitalcommons.bc.edu/cgi/viewcontent.cgi?article=1101&context=lsfp

[3] Balkin, Jack (2014). Information Fiduciaries in the Digital Age. *Balkanization*, 5 March. https://balkin.blogspot. com/2014/03/information-fiduciaries-in-digital-age.html

This Bill does not obligate data fiduciaries to always act in the best interest of data principals, except in one provision: processing of personal and sensitive data of children.[4] Instead, the Bill places higher expectations upon data principals and requires them to look out for their own interests.

At the same time, certain provisions enable excessive power concentration in the hands of the data fiduciary. As discussed in detail in the section on non-consensual processing of data of this submission, in a number of sections the Bill prioritises the interests of the State and employers at the expense of the right to privacy of data principals.

As further expanded on in the section on data access by the State in the current submission, the Bill authorises the Central Government in particular with excessive powers. The Central Government is empowered to process data without consent for various reasons. Lastly, the State is also empowered to appoint and remove the regulators and adjudicators in case of disputes.

Thus, the Bill has skewed the fiduciary relationship between the data fiduciary and data principal by favouring the data fiduciaries, thereby leaving data principals vulnerable to all kinds of privacy harms.

To truly build a fiduciary relationship, it is recommended that wherever arises in the Bill a question of balance of interest between a data principal and a data fiduciary (such as with regard to non-consensual grounds of processing personal data by employers; reasonable purposes of processing by private/state actors; non-consensual grounds of processing of personal data by the state actors; and exemptions, among others), the privacy of the data principal should be the first priority.

More concretely, we recommend changes are made to the following sections of the Bill:

- Section 12: Grounds for processing of personal data without consent in certain cases
- Section 13: Processing of personal data without consent for purposes related to employment
- Section 14: Processing of data without consent for other reasonable purposes
- Insert new section: The State is not a unitary entity
- Section 23: Consent manager
- Insert a new right, the right to object, in the chapter on data principal rights.
- Sections 11 and 21: Concerns affecting data principals' data protection rights
- Sections 35 and 36: Exemptions
- Social Media Verification
- Safe Harbor from data protection obligations while processing anonymised data:
- Section 91: access to non-personal data

[4] Chapter IV Section 16 (1), Personal Data Protection Bill, 2019.

Section 12: Grounds for processing of personal data without consent in certain cases

(a) Processing of personal without consent for functions of the State:

The relationship between the State and the citizen is unique, as the State is required to perform various functions for the proper functioning of the State and the benefit of the citizenry. The exercise of each of these functions requires the State to collect vast amounts of information about the citizens. Moreover, there are certain functions only the State can perform, such as issuing licenses and permits, subsidies and benefits, and formulating government schemes. In such situations it is difficult to actualise meaningful consent as a grounds for processing, as withdrawal of consent would mean exclusion from the goods, services or benefits offered by the government. Recognising this, several other jurisdictions, such as the E.U in the GDPR, have created 'exercise of public authority' as a separate ground for lawful processing other than consent.[5][6]

While it may, thus, be true that meaningful consent cannot always be obtained by the State at every instance, section 12 of the present Bill nevertheless is concerning because it provides for a blanket exemption to the consent requirement for the State under the garb of 'any function of the State'. This is particularly concerning seeing that the definition of the State,[7] according to this Bill, it is the same as defined under article 12 of the Constitution.

This definition includes the Central, State and local governments as well as any other authority under the control of the Government of India. Though the term 'other authority' is not defined in the Constitution, the Supreme Court has held that this is to be determined based on 'whether in the light of the cumulative facts as established, the body is financially, functionally and administratively dominated by or under the control of the Government.'[8] As a result of the liberal interpretation of this term, a range of bodies such as central/state universities, corporations and registered societies have, thus, been recognised as state.

Therefore, when section 12(a) is read with section 3(39), it appears that under the ambit of 'any function of the State', all 'other authorities' as per article 12 of the Constitution may process personal data without consent, for all economic, educational, and medical functions provided by them. This is far too wide a scope. There is no reason why consent should not be sought for services that are not essential for life and livelihood or can be provided by actors other than the State.

---

[5] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna (2018). A Free and Fair Digital Economy Protecting Privacy, Empowering Indians. New Delhi. July 2018. Ministry of Electronics and Information Technology, Government of India. https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf

[6] Refer to article (6) of the General Data Protection Regulation (GDPR).

[7] Chapter I Section 3(39), Personal Data Protection Bill, 2019.

[8] Pradeep Kumar Biswas v. Indian Institute of Chemical Biology, 2002 (5) SCC 111.

In light of the above, it is therefore recommended to narrow the scope of the meaning of the term state as well as to reduce the scope of 'any function of the state' to two particular kinds of functions, as recommended by the Srikrishna Committee: (i) provision of any service or subsidies in the nature of welfare benefits; and (ii) performance of regulatory functions.[9]

Moreover, from a bare reading of sections 12(a) and 12(b), it is not clear that 'any function of the State' has to be provided for by law, i.e. a statute or an executive order. Therefore, this section enables the State to assume its functions without legal backing and thus to process personal data without any legitimate purpose, making it a problematic provision.

(*b) Processing of data without consent for other functions:*

In addition to the above mentioned grounds, the Bill lays down certain other grounds for processing. One of the concerning clauses is clause (f) of section 12. The clause permits the data fiduciary to 'undertake any measure to ensure safety of, or provide assistance or services to, any individual during any disaster or any breakdown of public order.'

While it is true that situations of emergency require prompt action, and non-consensual processing of data would be necessary to respond promptly in such circumstances, inclusion of vague terms such as 'any breakdown of public order' is problematic.

This term has not been defined or restricted (for example in terms of their scale or the speed at which they are developing) and are prone to wide interpretation. Precedent has shown that vague terms have been a means to abuse the exercise of power through wide interpretations. For instance, 'public order' has been stated to be a reasonable restriction on the exercise of rights granted by the constitution, but precedent has shown how it has been interpreted to curb fundamental rights in numerous instances.[10]

In addition, clauses c, d, e and f under the section do not specify whether the processing for these functions can only be carried out by the State. Therefore it means that private actors can also process personal data without consent for these purposes. In the absence of specificity, this provides a slippery slope for private actors to process data without any consent requirement and may prove to be dangerous, specifically for clauses (e) and (f).

---

[9] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna (2018). A Free and Fair Digital Economy Protecting Privacy, Empowering Indians. New Delhi. July 2018. Ministry of Electronics and Information Technology, Government of India. Page: 111.
https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf

[10] Chandavarkar, Madhav (2016). In the Interests of public order. *Live Mint.* 23 February.
https://www.livemint.com/Opinion/5WLiRnhxwVIpeNKwSZ6XjN/In-the-interests-of-public-order.html

Recommendations:

- The scope of section 12 (a), 'any function of the State' should be narrowed down to two particular kinds of functions: (i) provision of any service or subsidies in the nature of welfare benefits; and (ii) performance of regulatory functions.
- Processing of data without consent for the provision of any service or benefit under Section 12 (a) subclause (1) should be strictly mandated by law or an executive order. The State shall take all necessary measures to ensure that such laws are explicitly necessary and proportionate to the required function
- The meaning of the State for this section should be narrowed down to the necessary central and state government departments required to perform the narrowed functions of the State mentioned above.
- The Bill should provide clarity with respect to the meaning of the term 'breakdown of public order'.
- A provision for the right to object, including the right to object to automated decision making, must be applicable to the State when it carries out any function under section 12(a). The scope and applicability of the right to object has been outlined in a later section of this submission.

Section 13: Processing of personal data without consent for purposes related to employment

A bare reading of section 13 makes it apparent that it is violative of the basic principle of a fiduciary relationship, wherein a fiduciary is required to abnegate its own personal interest to always act in the best interest of the beneficiary. This section enables employers to act only in their personal interest, while undermining the exercise of their rights by employees.

Section 13 empowers employers (data fiduciaries) to seek and process employees' (data principals) data without the consent from their employees (data principals) on the following grounds: recruitment/termination, provision of any service/benefit to the employee, for assessment of performance and verification of attendance.

As these grounds are vague, broad and ambiguous, they exacerbate the power imbalances that exist in an employer-employee relationship and allow employers to effectively conduct surveillance on their employees.

It is imperative to understand that there always exists a power imbalance in a 'employer-employee' relationship. An employee seeks cost of her livelihood, intellectual and creative satisfaction, among other things, from her employer on the basis of her employment contract; therefore until she finds another opportunity to fulfill these needs, she is significantly dependent on her employer, hereby further empowering the employer. Instead of addressing this existing imbalance, this Bill makes matters worse by empowering employers to process personal data of their employees without obtaining their consent.

It deserves to be noted here that deployment of sophisticated technologies to assess performance of employees does not necessarily have positive results. There are various studies that suggest that workplace surveillance restrains people from being productive.[11] Carl Botan found that workplace surveillance can increase workplace stress, promote worker alienation, lower job satisfaction, and convey the perception that the quantity of work one generates is more important than its quality.[12] Sally A. Applin and Michael D. Fischer[13] found that employee surveillance leads to the creation of a culture wherein 'people more often alter their behavior to suit machines and work with them, rather than the other way around, and that this has eroded conceptions of agency.'

Recommendation:

In light of these harms, section 13 should be omitted from the Personal Data Protection Bill. There should be no exemption for employers to process data. Instead, employers should be required to follow the same obligations as any other private data fiduciary under the Bill.

Section 14: Processing of data without consent for other reasonable purposes

This section lays down that certain additional grounds can be specified by regulations for processing of personal data without consent for 'other reasonable purposes'.

Section 14(1) empowers the Data Protection Authority to specify other reasonable purposes, after considering factors such as the interest of the data fiduciary, the effect of such processing on the data fiduciary, the public interest, and a reasonable expectation of consent. It is disconcerting that the interests of the data fiduciary are emphasised in this section. With this, this section, too, furthers the imbalance between data fiduciary and data principal.

In addition, the authority has been granted the power to determine whether the provision of notice under section 7 will be applicable or not, depending on the nature of the reasonable purpose. Given that the grounds for defining reasonable purposes prioritise the interest of data fiduciary, and not the interest of data principal, it is problematic to redact the obligations under section 7 in such a situation.

Moreover, considering that the authority is not an independent body and has an executive composition, and that the data fiduciary may well be the State, there may be instances of subjective discretion, making it additionally controversial.

---

[11] Aiello, John R and Kolb, Kathryn. J (1995). Electronic performance monitoring: A risk factor for workplace stress. In S. L. Sauter & L. R. Murphy (Eds.). *Organizational risk factors for job stress*. Washington DC: American Psychological Association. Page: 163-179. https://psycnet.apa.org/record/1995-98299-010

[12] Botan, Carl (1996). Communication work and electronic surveillance: A model for predicting panoptic effects. *Communication Monographs*, 63(4). Page: 293-313. https://doi.org/10.1080/03637759609376396

[13] Applin, Sally A and Fischer, Michael (2013). Watching Me, Watching You. (Process surveillance and agency in the workplace). IEEE International Symposium on Technology and Society (ISTAS): Social Implications of Wearable Computing and Augmented Reality in Everyday Life. Toronto. IEEE.Page: 268-275. https://ieeexplore.ieee.org/document/6613129

The grounds that have been included in section 14(2) are also overly broad, which once again contributes to strengthening the power of the data fiduciaries at the expense of the data principals.

'Prevention of unlawful activity' allows the Government to look at the citizens through a dangerous lens of 'presumption of guilt'. This is a problematic provision as it violates the principles of due process,[14] while at the same time providing law enforcement and other government agencies with almost unrestricted access to data.

Moreover, such processing is prone to amplify the biases embedded in the criminal justice system,[15] which result in unfair targeting. This is the case, for example, with technologies such as facial recognition software, that claim to be used for preventive purposes but are highly inaccurate, among a slew of other problems.[16] In addition to the opacity surrounding the use of such technologies, the mistaken belief that technology is neutral also makes it harder for decisions made by such technology to be questioned. Recourse then becomes difficult.

Similarly, if 'credit scoring' is accepted as a reasonable purpose, this too will be plagued by opacity. While traditional credit scoring comes with its own biases, in the age of datafication, big data analytics and AI tend to magnify these biases, further impacting the communities concerned.[17][18] It also deserves to be noted that companies have started to garner data across platforms, including from social media, to decide an individual's credit worthiness, going far beyond traditional metrics.[19] While credit scoring may help to ensure access to credit for some, seeing the intrusive data gathering it often entails, such scoring should be done with the consent of the individual concerned.

The reasonable purpose of 'operation of search engines' is a newly added, vague and very broad provision, with no explanation. Due to the lack of clarity, it may lead to ambiguity and leaves room for misinterpretation. For example, taking into account section 14(1)(a), a search engine may argue that to enhance its functionality and increase efficiency, it requires personal data of individuals for operation of the search engine. In an absolute sense, this may not qualify as a reasonable purpose, but when read in the light of section 14(1)(a), (b) and (c), this request may qualify as reasonable purpose, which is unsettling.

---

[14] Concerned Citizens (2018). Solving for data justice: A response to the draft Personal Data Protection Bill. New Delhi. October 2018. Internet Democracy Project. https://internetdemocracy.in/reports/datajustice/

[15] Singer, Natasha and Metz, Cade (2019). Many Facial-Recognition Systems Are Biased, Says U.S. Study. *New York Times.* 19 December. https://www.nytimes.com/2019/12/19/technology/facial-recognition-bias.html

[16] Staff Reporter (2018). Police facial recognition software inaccurate. *The Hindu.* 24 August. https://www.thehindu.com/news/cities/Delhi/police-facial-recognition-software-inaccurate/article24764781.ece

[17] Eveleth, Rose (2019). Credit Scores Could Soon Get Even Creepier and More Biased. *Vice.* 13 June. https://www.vice.com/en_us/article/zmpgp9/credit-scores-could-soon-get-even-creepier-and-more-biased

[18] Waddell, Kaveh (2016). How Algorithms can bring down Minorities' Credit scores. *The Atlantic.* 2 December. https://www.theatlantic.com/technology/archive/2016/12/how-algorithms-can-bring-down-minorities-credit-scores/509333/

[19] Yanhao, Wei and Yildirim, Pinar and Van den Bulte, Christoper and Dellarocas Chrysanthos (2015). Credit Scoring with Social Network Data. *Marketing Science*, 35(2): 234-258. http://dx.doi.org/10.1287/mksc.2015.0949

Another concerning purpose is 'processing of publicly available personal data'. There is no clarity on what constitutes publicly available personal data. Such ambiguity in the current text of the law could lead to profiling and targeting of individuals based on that profile. Furthermore, this would effectively put into place a legal ground for social media surveillance of all citizens, without consideration for due process,[20] and have a chilling effect on free speech and social interaction online.[21]

As rightly pointed out by the Sri Krishna committee report while addressing this provision: 'While an individual making personal data public may have a lower expectation of privacy, it is unlikely that every kind of disclosure is made with the expectation that personal data may be used for profiling whether by private entities or by the State.'[22] Such broad-based exemptions are therefore inappropriate in a Personal Data Protection Bill.

Recommendations:

- Section 14 should strengthen the fiduciary relationship. Therefore section 14(1)(a) should be omitted, and 14(c) should be redrafted to read 'any compelling public interest in processing for that purpose without overriding the fundamental rights and freedoms of the data principals'.
- Processing on the grounds of 'prevention and detection of any unlawful activity including fraud', 'credit scoring', 'publicly available personal data' and 'the operation of search engines' need to be omitted from the provision.
- Section 14(3)(b) should be redrafted to ensure that the provisions of notice under section 7 shall apply by default, with the Authority being granted the power to determine exceptions in such cases where such provision shall substantially prejudice the relevant reasonable purpose.
- In cases where the notice under section 7 shall apply, the data principal must have the right to object, including to profiling and to automated processing. These rights have been further discussed in detail in a later section of this submission.

Insert new section: The State is not a unitary entity

At present, the Bill treats the State as unitary. A bare reading of sections 12 and 14 makes it apparent that, there are no restrictions in the Bill on the extent to which or conditions under

[20] Shahbaz, Adrian and Funk, Allie (2019). Freedom On The Net 2019: The Crisis of Social Media. Washington, DC. Freedom House. https://www.freedomonthenet.org/sites/default/files/2019-11/11042019_Report_FH_FOTN_2019_final_Public_Download.pdf

[21] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna (2018). A Free and Fair Digital Economy Protecting Privacy, Empowering Indians. New Delhi. July 2018. Ministry of Electronics and Information Technology, Government of India. https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf

[22] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna (2018). A Free and Fair Digital Economy Protecting Privacy, Empowering Indians. New Delhi. July 2018. Ministry of Electronics and Information Technology, Government of India. https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf

which intergovernmental sharing of data is allowed: data gathered by one arm of the State, for a specific purpose, can be accessed by other arms of the State, including those concerned with law enforcement, without violating any of the provisions of the Bill.[23]

This is rather different from, for example, the Estonian model,[24] in which the citizen is in control of what data is being shared amongst various state agencies, in addition to the consent of the citizen being required before any processing. In order to ensure transparency and accountability, citizens can inquire which agency has accessed their data. Any instance of overstepping by a Government agency can lead to an investigation.

Transparency and accountability are key to any democratic functioning and should be reflected in a data protection regime in India as well. This can happen only through strong legal safeguards against abuse and equally strong rights that can be meaningfully enforced.

Recommendations:

To strengthen the fiduciary relationship, and instill the trust of beneficiaries (data principals) back in the State, it is recommended that:

- A provision be inserted in the Bill to prevent intergovernmental sharing of data between the State or any of its agencies without consent of the data principal.
- The requirement of consent only be done away with in exceptional circumstances, i.e. when providing medical aid or assistance under clauses (d), (e) or (f) of section 12.
- The State additionally devises a mechanism to ensure that data principals (citizens) are able to know which state agency is the main controller of a particular set of their data, what data they have, and with whom this data is being shared at any given point of time.

Section 23: Consent manager

The explanation clause of section 23 of the Bill provides for a technical solution to operationalise and manage consent in the form of a tool called a 'consent manager'. From a bare reading of the Bill, it appears that the consent manager can be a separate data fiduciary, or an already existing

[23] Support for this approach can also be found in policy documents such as the Economic Survey 2018-2019 which advocates for a creation of a 'Centralised Welfare Based Database for citizens' by merging different databases maintained by separate Ministries and departments. The survey goes on to back this by reasoning that one must not impose the 'elite's preference of privacy on the poor, who care for a better quality of living the most.' Furthermore, data may also be made available to private agencies for commercial purposes. See Department of Economic Affairs, Ministry of Finance (2019). Economic Survey (2018-219) Volume 1. Chapter 4: Data "Of the people, by the people, for the people". New Delhi. February 2019. Ministry of Finance, Government of India. https://www.thehinducentre.com/resources/article28283388.ece/binary/Economic%20Survey%20Volume%20I%20Complete%20PDF.pdf

[24] Priisalu, Jane and Ottis, Rain (2017). Personal control of privacy and data: Estonian experience. *Health and Technology*. Page: 441–451. https://doi.org/10.1007/s12553-017-0195-1

data fiduciary which is required to register itself with the Authority to allow data principals to gain, review, withdraw and manage their consent.

In theory, this technological solution might appear to be a silver bullet, however there are several issues with this proposal.

This Bill proposes a 'notice and consent' model and therefore consent becomes one of the central components of the Bill. Unfortunately, however, the Bill fails to provide any clarity on the privacy framework that is to be adopted by consent managers to operationalise individual consent. While it may not be possible to lay down detailed specifications to be observed by the consent managers in the Bill, at least the scope and role of the consent managers should be provided within the Bill and should not be left upon delegated legislation which is merely an executive decision with insufficient parliamentary insight.

Further, a consent manager is a technological solution that is intended to make the exercise of consent more convenient. However, this tool comes with its own set of risks, including risks of profiling, manipulation, surveillance and targeted delivery of ads, among others. Unfortunately, the Bill fails to provide the additional obligations for those data fiduciaries that may assume the role of consent managers.

For example, every transaction through a consent manager would lead to the creation of personal data and a set of metadata.[25] Access to this personal data and metadata would mean that a data fiduciary (consent manager) would have considerable insight into all the data-based decisions made by a data principal using the consent manager. Thus, if a person buys a product online using a credit/debit card, the consent manager would know about the name of the person buying the product, and in some cases even the gender of the person, the marketplace from where the purchase has been made, the name of the bank that has been used to buy the product, the type of card used, the product or service being accessed and the time and location of purchase. Moreover, the consent manager would collect such data for every transaction. However, in its present version, the Bill does not prevent such information from being used by the consent manager for use cases such as targeted profiling/selling data, among others.

Similarly, if the State or a state agency becomes a consent manager, there is nothing in the Bill that stops the metadata from being used for mass surveillance.

Recommendations:

The Bill should provide clarity with respect to the scope and role for the proposed consent manager by providing clarity regarding the following questions:

[25] Metadata may be defined as secondary data about primary data, for example in case of online messaging, metadata would include every other data apart from the actual message i.e. data about parties, time, location among others. See International Committee of the Red Cross (ICRC) and Privacy International (2018). The humanitarian metadata problem: "Doing no harm" in the digital era. Geneva, ICRC and Privacy International. https://privacyinternational.org/sites/default/files/2018-12/The%20Humanitarian%20Metadata%20Problem%20-%20Doing%20No%20Harm%20in%20the%20Digital%20Era.pdf

- whether any data fiduciary can assume the role of consent manager,
- whether consent managers can also be called as significant data fiduciaries.

Furthermore, there should be certain additional obligations within the law to prevent misuse of personal data by the consent manager, in particular:

- It may not use any personal or non-personal data, including meta data collected, for any other purpose apart from managing consent.
- It should be data blind when a data exchange is taking place between data principal and data fiduciary for a specific purpose.
- It should deploy a decentralised method to operationalise this tool.
- It should not be allowed to sell or share any personal or non personal data collected with any other data fiduciary including the State.

Insert a new right, the right to object, in the chapter on data principal rights.

Jurisdictions around the world have included various next generation rights in their data protection legislation. While this Bill provides certain rights to the data principal, next generation rights are excluded from this Bill. These include the right to object, the right to object to decisions solely based on automated decision making and the right to object to processing for the purpose of direct marketing. Such rights are intended to specifically address the asymmetry of power between people and entities in large-scale data processing.[26] Their exclusion from this Bill is detrimental to the data principal's ability to exercise agency in the age of AI and big data analytics in particular, further skewing the power imbalance in favour of the data fiduciaries.

While analysing the applicability of these crucial next generation rights in the Indian scenario, the Justice Sri Krishna Committee report argued that the problems related to large scale processing of data should not be dealt with by individuals; rather the responsibility should lie upon the data fiduciaries and the Data Protection Authority.[27] More concretely, the Justice Sri Krishna Committee report prescribed an ex-ante framework to ensure accountability (for instance, by strengthening privacy designs, auditing and review) to deal with the issues that arise from automated decision making, instead of adopting rights which address automated decision making.[28] It also stated that the individual can always approach courts in case a problem arises.

However, in a scenario where the data fiduciaries happen to be the State or a powerful MNC, it is vital for data principals to be equipped themselves with tools to unearth and challenge any

---

[26] Ranganathan, Nayantara (2018). India's data protection draft ignores key next-generation rights. *Asia Times.* 9 August. http://www.atimes.com/indias-data-protection-draft-ignores-key-next-generation-rights/

[27] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna (2018). A Free and Fair Digital Economy Protecting Privacy, Empowering Indians. New Delhi. July 2018. Ministry of Electronics and Information Technology, Government of India. Page: 73-74
https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf

[28] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna (2018). A Free and Fair Digital Economy Protecting Privacy, Empowering Indians. New Delhi. July 2018. Ministry of Electronics and Information Technology, Government of India. Page: 74-75.
https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf

potential harm arising from such processing as well. This becomes even more critical in this Bill since the independence of the Data Protection Authority, as per the current provisions of the Bill, is also in question.

Moreover, the drive towards data-governance means that important decisions that can impact the quality of an individual's life can be automated; but large scale processing is often marked by opaque decision making, and human biases percolate down into systems such as A.I. In such cases, too, next generation rights are crucial tools to ensure justice to data principals. Where harm is suspected to have been done, approaching courts might lead to time-lags, possibly causing more harm in the process.

The Bill provides an opportune moment to truly empower the data principals through these rights in an age of large scale data processing.

(a) Right to object

The right to object is not an absolute right. It can be exercised on certain grounds and subject to certain conditions. Article 6(1)(e) and 6(1)(f) of the EU's GDPR grants people the right to object to the processing of their personal data, subject to their particular circumstances, on the following grounds: 'performance of a task carried out in public interest' or in the 'exercise of public authority which is laid down in law', or on the ground of pursuance of legitimate interests by the controller or third party.[29][30] When a data subject exercises her right to object, the controller has to stop processing the data unless the controller can demonstrate a compelling legitimate interest for processing of the said data which overrides the interests, rights and freedoms of the data subject. Thus, this right shifts the burden of proof onto the data controller from the data subject.

The current draft of the Personal Data Protection Bill should similarly provide this right to data principals for instances wherein their personal data is being processed without consent (in cases where personal data is processed within the consent and notice framework, the data principal can instead opt-out of such processing by withdrawing their consent). The Bill should incorporate the right to object against both the State and private entities.

The Sri Krishna Committee report had argued that it would be difficult to adopt this right in the Indian context given that the Personal Data Protection Bill's framework and grounds of processing are different from that of the E.U's GDPR.[31] However, a granular reading indicates that the grounds for processing for 'performance of task carried out in public interest or or in the exercise of official authority vested in the controller'[32] refers to functions similar to those that

[29] Refer to article 6 of the GDPR.
[30] Refer to article 21 of the GDPR.
[31] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna (2018). A Free and Fair Digital Economy Protecting Privacy, Empowering Indians. New Delhi. July 2018. Ministry of Electronics and Information Technology, Government of India. Page: 73-74.
https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf
[32] Refer to article 6 (1) (e) of the GDPR.

are to be undertaken by the State under section 12(a). Similarly, section 14 provides for processing on the grounds of 'other reasonable purposes'; this refers to the grounds for processing covered under 'legitimate interests by controller or third party' of the GDPR.

Recommendations:

- A right to object to processing under sections 12(a) and 14 of the Bill should be inserted in Chapter VI, on Data Principal Rights, of the Bill, enabling data subjects to object to the processing of data by both the State and other data fiduciaries, subject to their particular situation.
- The provision should clarify that if the data fiduciary refused to entertain the request by the data principal to exercise this right, the data fiduciary will be required to demonstrate compelling grounds for processing which override the interests, freedoms and rights of the individual or that the said processing was necessary for the establishment, exercise or defence of legal claims.

(b) Right to not be subjected to decisions solely based on automation

The EU's GDPR under Article 22 provides data subjects with a right not to be subject to decisions solely based on automation, including profiling, which produce legal effects concerning the individual or similarly significantly affect the data subject.

The right does not apply (a) when the decision is necessary for performance of a contract; (b) when the automated decision making is authorised by law of a member state; or (c) when explicit consent was given. However, even if these grounds are used to justify processing, the data controller still has to implement suitable measures to safeguard the data subject's rights, freedom and legitimate interests under article 22 (3) of the GDPR.

With increasing use of data-driven governance models and sophisticated algorithms by private entities, big data and A.I are being used increasingly used by the State and private entities alike to make decisions that have profound implications on people's lives. For example, individuals have been denied housing, credit, and employment opportunities due to automated decisions, causing extreme hardships.[3334] The impact is greater for vulnerable sections of societies whose quality of life can decrease significantly as a result of a denial of essential services and opportunities.[35] The inclusion of this right would enable data principals to exercise agency by providing them the avenue to raise objections in case they are subject to the risks that arise from profiling and opaque automated decision making. Even in cases where the automation would not

[33] Eubanks, Virginia (2018). *Automating Inequality: How High Tech Tools Profile, Police and Punish the poor*. New York. St. Martin's Press.
[34] O'Neil, Cathy (2016). *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. Portland, OR. Broadway Books.
[35] The Wire Staff, (2018). Of 42 'Hunger-Related' Deaths Since 2017, 25 'Linked to Aadhaar Issues. *The Wire.* 21 September. https://thewire.in/rights/of-42-hunger-related-deaths-since-2017-25-linked-to-aadhaar-issues

entirely stop, this right would allow for the data principal to seek human intervention or a reconsideration of their processing.

Recommendations:

- A right to object to decisions made under sections 12(a) or 14 of the Bill and based solely on automation, including profiling, should be inserted in Chapter VI, on Data Principal Rights, of the Bill, where such decisions can cause significant harm[36] to the quality of life of a data principal.[37]
- The provision should further clarify that, in cases where the decision-making is based on processing allowed by law, the data fiduciary needs to take suitable measures to ensure that the rights and freedom of the data principal are safeguarded. At a minimum, this would include a right to seek human intervention whenever a data principal's data is being processed solely on the basis of automation, and reconsideration of the decision if need be.

(c) Right to object to processing for the purposes of direct marketing:

This right, also included in the GDPR, allows an individual to object to the processing of personal data, including profiling, when it is related to direct marketing.[38] It is an absolute right, which means that the data fiduciary needs to stop processing immediately. Exercising this right enables an individual to protect herself against targeted advertisements and online profiling.

Recommendation:

An absolute right to object to processing for the purposes of marketing should be added to Chapter VI, on Data Principal Rights, of the Bill.

Sections 11 and 21: Concerns affecting data principals' data protection rights

This Bill aims to protect the personal data of individuals and their right to privacy. To operationalise this intent, the Bill empowers the data principal with certain rights.[39] However, there are certain conditions specified in the Bill which undermine any potential protection such rights might provide.

Specifically, section 11(6) of the Bill shifts the burden from the data fiduciary to the data principal when the data principal decides to withdraw her consent from the processing of any personal data without any valid reason. It states that 'all legal consequences' for the effects of such withdrawal shall be borne by the data principal. This puts a disproportionate burden on the data principal.

---

[36] Harm as defined under Chapter 1 section 3 (20), Personal Data Protection Bill, 2019.
[37] Including but not limited to obtaining welfare services, access to opportunities via employment, education amongst others.
[38] Refer to article 21 (2) of the GDPR.
[39] Chapter V Section 17, 18, 19, 20, 21, Personal Data Protection Bill, 2019

Recommendation:

Since the ease of withdrawal of consent is not comparable to the ease with which consent was taken, this provision needs to be omitted.

Section 21 (2) of the Bill states that in order to comply with any request made by the data principal for erasure, access data, update information, and portability among others, the data fiduciary may charge a fee. The fee discussed herein and the basis on which it would be decided has been left to delegated legislation. This makes it a concerning provision as India is trying to digitise all essential paper documents and identities.[40] If the correction, manipulation and updation of the data comes at a cost, considering the socio-economic fabric of India not every person will have adequate resources to bear this cost of privacy, and as a result all such people will be directly excluded. Further, this provision may not only lead to a privacy harm; if the personal data is incorrect and a person cannot afford the cost of updating, she may be excluded from accessing ration or medical aid, among other necessities, thus affecting a range of other rights.

Recommendations:

To prevent the creation of a system of exclusion, it is recommended that the Bill should delineate the following to empower every data principal:

- No cost/nominal fee would be imposed to update, access, correct, erase or port personal data to access services provided by the state as constitutional obligation to ensure that there is no violation of fundamental rights[41] that are read in the right to life;
- Services for which a fee may/may not be charged; and
- Categories of people such as marginalised/underprivileged communities which may be exempted to pay the fee to avail the services.

Sections 35 and 36: Exemptions

While it is the sovereign function of the State to ensure security of the State, it is imperative to note that in a democracy, this goal cannot be achieved by rolling out mechanisms for mass surveillance. In fact, a citizen-centric personal data protection legislation must provide strong safeguards against state surveillance.

However, not only is the current Bill silent on matters related to surveillance reforms, it rather actively enables a surveillant state through the wide exemptions given to the Government, through sections 35 as well as 36. In the absence of reforms, the exemptions proposed under

[40] Aadhaar, Pan card and Passport among others.
[41] Unni Krishnan v. State of A.P. 1993 AIR 217, 1993 SCC (1) 645, M.C. Mehta v State of Tamil Nadu & Ors (1996) 6 SCC 756 and, Mohini Jain v State of Karnataka 1992 AIR 1858, among others.

section 35 or 36 will be disastrous for the individual's right to privacy, as well as possibly affecting a slew of other rights.

(a) Section 35

Comprehensive reform of India's surveillance architecture has been called for from numerous quarters for at least a decade now.[42] At the very least, critics have argued, the following reforms should be put into place if India's surveillance architecture is to be worthy of a democracy:

- Statutory mandate for establishing intelligence agencies/security of the state agencies: all intelligence agencies, which currently are mostly established merely on the basis of an executive order, are provided statutory backing.[43] Further, these agencies shall only conduct activities as prescribed by a statute.
- Oversight mechanism: most of the Central/State intelligence agencies in India currently lack a proper oversight mechanism; they merely report to the executive department that established the agency. Thus, in addition, parliamentary and/or judicial oversight of all surveillance agencies and activities should be put into place.

In a democracy, aforementioned reforms should be the minimum standards of safeguards that should be put into place. In addition, robust legal safeguards against abuse specific to different situations and legislations and upholding equally strong rights should be enforced.

At present, however, none of these safeguards or minimum standards have been put in place in India.

On the contrary, section 35 of the Bill empowers the Central Government to exempt any government agency from application of all or any of the provisions of the Bill. This is a draconian section, unbecoming of a democratic country, which was not present even in the 2018 version of the Bill and considerably broadens the scope of the power of the Central Government.

The section enables not just notified intelligence or security agencies but any agency of the Central Government, on the order of the Central Government, to be exempt from any or all the provisions of the Bill. This is a disconcerting provision, because it enables unfettered executive overreach. These concerns are further heightened because of the absence of any judicial or parliamentary oversight. Moreover, there is no obligation upon the Central Government to notify the public about the agency that the Central Government is exempting under this section. Thus, this section is violative of the fundamentals of a democracy.

---

[42] See, e.g., Institute for Defence Study and Analyses (2012). A Case for Intelligence Reforms in India. IDSA Task Force Report. New Delhi. Institute for Defence Study and Analyses https://idsa.in/system/files/book/book_IntellegenceReform.pdf; Joshi, Manoj and Das, Pushan (2015). India's Intelligence Agencies: In Need of Reform and Oversight. ORF Issue Brief No. 98. New Delhi. July. Observer Research Foundation. https://www.orfonline.org/wp-content/uploads/2015/07/IssueBrief_98.pdf

[43] News 18, 2017. Right to Privacy Ruling: Intelligence Agencies That May be Affected. *News 18*. 24 August. https://www.news18.com/news/india/right-to-privacy-ruling-the-intelligence-agencies-that-may-be-affected-1499983.html

The Bill permits the exemption not just in the interests of security of the State, as section 42 of the earlier 2018 draft sought to do, but also adds the following grounds for the State to seek exemption: (i) in the interest of interest of sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order; or (ii) for preventing incitement to the commission of any cognizable offence relating to sovereignty and integrity of India, the security of the state, friendly relations with foreign states, and public order.

Further, the present Bill does not contain any requirement of legality, necessity, or proportionality, creating room for judicial interpretation. The Bill should explicitly include the Puttaswamy test laid down in the language of the Bill itself.[44]

In the absence of robust surveillance reforms, the current draft of Section 35 empower the State/Central Government with exceptional authority, and poses an imminent threat to the fundamental right to privacy of a citizen.

Recommendations:

No exemption can be given to the State in the name of security of the State, among other interests, without explicitly underpinning surveillance reforms. These should at the very least include:

- Statutory backing of all intelligence agencies, with these agencies only conducting activities as prescribed by the statute.
- Parliamentary and/or judicial oversight of all surveillance agencies and activities.

Only when these broader surveillance reforms have been put into place would it be appropriate to include in the Bill exemptions for the State that may enable it to surveil data principals on grounds of security of the State.

Even then, however, in order to ensure that data principals' rights are protected as appropriate in a democracy, section 35 would need to be redrafted along the following lines:

- The Central Government may exempt certain agencies (backed by statute) from application of certain provisions (mentioned below, in the recommendations on safeguards and oversight mechanism) and *not* all provisions of the Act.
- The Central Government may exempt any agency only if it is satisfied that it is necessary and proportionate to do so in the interest of 'security of the State'.
- There must be an order for an exemption, and reasons for such an order are to be recorded in writing.
- The order shall direct that certain provisions of the Personal Data Protection Bill[45] will not be applicable to certain agencies of the Government, backed by statute,

[44] Parsheera, Smriti (2020). Facial recognition technologies in India: Why we should be concerned, *LEAP Blog*. 3 January. https://blog.theleapjournal.org/2020/01/facial-recognition-technologies-in.html

[45] Chapters II (except for Sections 4, 5, 6, 9), III (except for Section 12), IV, V, VI (except for Sections 22, 24, 25, 30, 32), VII.

in respect of processing of such personal data as prescribed in that statute, subject to such procedures as prescribed by the same statute from which the agency derives authority.

Moreover the agencies shall be subject to certain safeguards and oversight mechanism while processing personal data under this section, as follows:

- An order under this Section should only be passed by an officer not below the rank of Secretary to the Government of India specially authorised in this behalf by an order of the Central Government.
- Each of these orders should be subject to judicial oversight, as recommended by the Supreme Court in the Aadhaar judgment:[46] judicial officers shall examine the validity of the order and prima facie case against the data principal.
- All orders issued under the Section should contain reasons for such direction, and a copy of such order should be made available to the for judicial officer to assess the legality of the order.
- When the Judge is of the opinion that the orders are not in accordance with Section 35, they should be empowered to set aside the directions and pass necessary consequential orders.

Further, the following safeguards, among others, included already in the Bill, should be incorporated in Section 35 as well:

- Even with the invocation of Section 35, the government agency should still be required to comply with certain basic requirements under the Bill, such as those under Sections 4, 5, 6, 9, 12, 22, 24, 25, 30, 32 and Chapters I, IX-XIV of the Bill.
- The Justice Srikrishna Committee in its report[47] provided that a personal data breach must be notified to data principals directly, not only when it poses harm to the data principals but also where some action is required on part of the principals to protect themselves from the consequences of the breach. This threshold should be adopted in the current Bill, and in all such cases the State should directly inform the citizens, rather than merely inform the Data Protection Authority.
- Personal data processed for any of the law enforcement purposes must be kept for no longer than is necessary for the purpose for which it is processed.

Only after prescribing robust surveillance reforms have been prescribed may the Bill lay

[46] K.S. Puttaswamy v Union of India, (2019) 1 SCC 1, para 447.
[47] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna (2018). A Free and Fair Digital Economy Protecting Privacy, Empowering Indians. New Delhi, 27 July 2018. Ministry of Electronics and Information Technology, Government of India.
https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf

down an exemption for security of the State, in the manner prescribed above.

(b) Section 36

This section exempts a data fiduciary from various provisions of the Bill[48] for processing of personal data for certain purposes delineated under the section.

Following are the interests that are too broad and widen the asymmetrical relationship between the data fiduciaries and the data principals in a dangerous way.

Section 36(a) allows exemption for processing of personal data in the interest of the 'prevention' of any offence or contravention of any law in force. Contrary to the traditional principle of 'presumption of innocence', this provision thus allows the Government to look at the citizens through a dangerous lens of 'presumption of guilt'. There exists sufficient evidence that proves that simply by belonging to certain communities, individuals have been disproportionately impacted.[49] This provision further exacerbates such harms.

As explained above, section 36(a) exempts data fiduciaries, including law enforcement agencies, to process personal data in the interest of 'prevention, detection, investigation, and prosecution of any offence'. The section does not, however, provide clarity on the instances where a data fiduciary (state or non state actor) may begin or continue processing of the personal data mentioned under this section. There is no safeguard or oversight mechanism prescribed within the exemption to prevent a data fiduciary to begin or continue processing data in the section; offences and punishments are the only recourse, which is insufficient. In the absence of more stringent safeguards, this provision can prove to be dangerous.

Section 36(b) allows data fiduciaries to seek exemption under the section for the processing of personal data for the enforcement of or for defending any legal right or claim, relief, or legal service. This is another very broad provision, as legal right or claim can mean even a contract for sale, among others. The Bill fails to provide a minimum threshold to bring this provision in action, which may prove to be problematic.

Recommendations:

- To ensure that data fiduciaries do not misuse section 36(a) and 36(b), the Bill should prescribe that the offence should be a cognizable offence and should be punishable with imprisonment upto 3 years as per the Indian Penal Code, 1860, for the data fiduciary to claim exemption under section 36(a). Similarly, to seek exemption under section 36(b), the Bill should prescribe that the exemption may be claimed for enforcing fundamental rights as well as for seeking relief, defending charge, or opposing claim, that may cause harm to the data principal.
- In addition, the word 'prevention' should be omitted from the interests mentioned

[48] Chapter except section 4, Chapter III to V, Chapter VI except Section 24, and Chapter VII.
[49] Satish, Mrinal (2010). 'Bad Characters, History Sheeters, Budding Goondas and Rowdies': Police Surveillance Files and Intelligence Databases in India. *National Law School of India Review*. 23(1). Page 133-154. https://ssrn.com/abstract=1703762

under section 36(a) of the Personal Data Protection Bill.

- To ensure that data fiduciaries do not start or continue processing personal data of individuals for the interests specified under section 36(a), a provision of judicial oversight should also be there for data fiduciaries to avail the exemptions under section 36(a).
- The particular agency undertaking the operations mentioned in section 36(a) should be required to comply with sections 5, 6, 8 and 9 of Chapter II of the Bill, which impose obligations on the data fiduciary relating to purpose limitation, collection limitation, ensuring quality and restriction on retention of data. The obligation to ensure the reporting of breaches (section 25) must also be applicable.

Section 28: Social Media Verification

Section 28 of the Bill obligates all social media intermediaries which may be notified as significant data fiduciaries to enable their users to voluntarily verify themselves in a prescribed manner. However, there is no clarity on how this may help users in ensuring their personal data protection, and for this reason, this provision is misplaced in a data protection Bill.

Moreover, by giving the impression that verification somehow aids data protection, the Bill inappropriately discredits the value of the principle of anonymity, which elsewhere has been recognised as a central aspect of the Internet and privacy.[50]

In addition, and contrary to the objectives of the Bill, the provision facilitates and encourages the collection of even more personal data by social media intermediaries from individuals, even when this is not required to provide the desired services. The section thus violates the principle of purpose limitation included in the Bill.

Furthermore, there is evidence from other instances that social media intermediaries have misused data provided by users in good faith in order to keep them 'safe' to serve users targeted ads. For example, social media intermediaries have misused 2FA (two factor authentication data) to profile and serve advertisements to their users.[51]

Finally, concerns about this provision are further heightened by the widespread access to data that the State is granting itself under this Bill and in various draft regulations currently under discussion, including the draft Intermediary Guidelines (Amendment) Rules 2018. Those who opt in to such verification make themselves vulnerable to even deeper surveillance by the Indian State, again undermining the protection of their personal data, rather than strengthening it.

---

[50] ARTICLE 19 (2015). Policy Brief: Right to Online Anonymity. London. United Kingdom. ARTICLE 19. https://www.article19.org/data/files/medialibrary/38006/Anonymity_and_encryption_report_A5_final-web.pdf

[51] Lomas, Natasha (2018). Yes Facebook is using your 2FA phone number to target you with ads**,** *Tech Crunch*. 27 September. https://techcrunch.com/2018/09/27/yes-facebook-is-using-your-2fa-phone-number-to-target-you-with-ads/

While the provision stipulates that verification is voluntary for now, we have seen on other occasions how initiatives that were voluntary initially later became mandatory - Aadhaar being a prime example. If social media verification is going to follow the same route, this will further facilitate the tracking of the entire Indian population's user behaviour online in unprecedented ways. Among many other effects, this would likely have a chilling effect on free speech and therefore would be violative of the fundamental right to freedom of expression.

Recommendation:

This provision should be omitted from the Personal Data Protection Bill.

Safe Harbour from data protection obligations while processing anonymised data:

Provisions of this Bill do not apply to anonymised data. Section 2(B) of the Bill provides safe harbor protection to data fiduciaries from the Bill for processing of anonymized data. Anonymised data is defined as "personal data that has been through the anonymisation process leaving it untraceable from the body that it has been retrieved from".

This is a problematic provision. It is imperative to note that there is no such thing as bulletproof anonymisation.[5253] For example: a journalist and a data scientist unveiled the ease with which they could re-identify individuals from anonymized browsing history (URLs) of three million German citizens. They claimed that merely ten URLs are enough to identify an individual uniquely by drawing parallels with other easily available public data (such as social media accounts, public YouTube lists among others).[54] This implies that despite applying robust standards for anonymisation, data can easily be traced back to its originating body from an anonymised dataset.[5556]

The Bill fails to acknowledge that an anonymised data set can be easily re-identified and therefore it does not recognise re-identification of anonymised data as an offence. Section 82 of the Bill only recognises re-identification of de-identified dataset as an offence. This is inadequate to protect individuals from the risks of re-identification from anonymised data.

---

[52] Narayanan, Arvind and Felten, Edward W (2014). No silver bullet: De-identification still doesn't work. 9 July. https://www.cs.princeton.edu/~arvindn/publications/no-silver-bullet-de-identification.pdf

[53] Rocher, Lue and Hendrickx, Julien.M. and de Montjoye, Yves Alexandra (2019). Estimating the success of re-identifications in incomplete datasets using generative models. *Nature Communications 10,* 3069. https://doi.org/10.1038/s41467-019-10933-3

[54] Hern, Alex (2017). 'Anonymous' browsing data can be easily exposed, researchers reveal. *The Guardian*. 1 August. https://www.theguardian.com/technology/2017/aug/01/data-browsing-habits-brokers

[55] In 2014, an anonymised Netflix dataset of film ratings was deanonymised by comparing the ratings with public scores on the IMDb film website in 2014, revealing the identities of individuals, their sexual identities and other sensitive person information.

[56] Ohm, Paul (2010). Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA Law Review.* 1701. http://paulohm.com/classes/techpriv13/reading/wednesday/OhmBrokenPromisesofPrivacy.pdf

Recommendations:

- Blanket safe harbor from data protection obligations should not be granted to data fiduciaries while processing anonymised data. Instead, data fiduciaries should be mandated to observe the data fiduciary obligations as laid down under Chapter II and security safeguards as delineated under Chapter VI of the Bill when processing anonymised data as well.
- Moreover, there should be an addition of offence under section 82: intentionally or knowingly de-identifying anonymized data should be recognised as an offence under this section.

Section 91: access to non-personal data

Section 91(1) of the Bill empowers the Central Government to draft policies for the digital economy that do not concern personal data. As this is a personal data protection Bill, any provision which is not in line with that purpose is misplaced; this includes section 91(1).

Recommendation:

Section 91(1) should be dropped from the Bill.

Section 91 (2) of the Bill enables the Central Government to access non personal data from any data fiduciary or data processor to enable better targeting of delivery of services or formulation of evidence-based policies by the Central Government.

It is pertinent to note that a non-personal data committee of experts[57] has already been constituted under the chairmanship of Shri Kris Gopalakrishnan, to discuss the issues and matters concerning non-personal data. The constitution of this committee is an important acknowledgement of the fact the challenges surrounding non-personal data are in a league of their own, and deserve thorough policy attention in their own right. Before related provisions are included in any legislation, it is imperative that much wider consultations and discussions on this important topic take place. Formulating legislation before this has happened is deeply inappropriate.

In addition to the above, there are several substantive reasons why this provision is deeply problematic.

While defining 'non personal data', the Bill adopts the same approach as prescribed under GDPR i.e. there is no clear and exhaustive definition of non personal data.[58] Instead, in the explanation

[57] Ministry of Electronics and Information Technology (2019). Constitution of a Committee of Experts to deliberate on Data Governance Framework. Office Memorandum No. 24(4)/2019 CLES. New Delhi. 13 September 2019. Ministry of Electronics and Information Technology, Government of India. https://meity.gov.in/writereaddata/files/constitution_of_committee_of_experts_to_deliberate_on_data_governance_framework.pdf

[58] Forge, Simon (2018). Optimal Scope for Free-Flow of Non-Personal Data in Europe, PE 618.988. Briefing required by IMCO Committee. Policy Department for Economic, Scientific and Quality of Life Policies. Brussels.

to section 91, the Bill states that all data which is not personal is termed as non personal data. However, in most cases personal and non personal data are collected together and it is very difficult to separate the two. Further, de-identification studies have shown that demographic data points can also lead to the identification of individuals. Therefore, due to lack of robust definitions and mechanisms, blanket access to non personal data from private entities poses a privacy risk to individuals.

From the anonymisation debate we have learnt that it is increasingly tough to truly anonymise data as there exist algorithms and statistical methods that enable re-identification of anonymised data.[59] This implies that since there is no such thing as perfect 'anonymisation', anonymised data cannot be simply termed as 'non-personal data' and no non-personal dataset should be relinquished to the Central Government.

In fact, in the absence of strong protections of citizens' rights, such as the duty to ask for consent for this kind of processing and/or the inclusion of a right to object to it, this provision further undermines the fiduciary relationship between the State and data principal as it once again excessively empowers the State to control the data of its citizens.

It is further imperative to note that the non-personal data to be collected under this provision would be used to devise Central Government policies, schemes and services. However, private entities have limited data sets as different private players have different data principal bases. In addition, the data that they collect and aggregate is for a specific purpose, which may differ in important ways from the policy challenge that the Central Government is seeking to solve through a particular policy, scheme or service. Moreover the datasets constructed by private entities would also be colored by the biases that the private entity may have fed in while processing data for its own use. As a result, any decisions that the Central Government would be making on the basis of such a dataset would further replicate these biases into the socio-political and socio-economic policies, schemes and services of the country. Therefore, in the absence of a much more extensive regulation on non-personal data that takes these manifold complexities into account, this provision would lead to the accumulation of biased non-personal data in Government hands, and thus to the violation of the fundamental rights to privacy and to equality.

This provision can also give rise to the creation of non-personal data exchange portals or mechanisms which would impact individual rights over data. In the past, the Ministry of Road Transport and Highways sold the *Vahan* and *Sarathi* databases to private and government entities for money.[60] Though the Bill does not provide for further sale of data acquired by government agencies under section 91, no provision of the Bill prevents the government from

---

IMCO Committee.
http://www.europarl.europa.eu/RegData/etudes/BRIE/2018/618988/IPOL_BRI%282018%29618988_EN.pdf

[59] Refer to "Safe Harbor from data protection obligations while processing anonymised data" section.

[60] Singh, Varun (2019). Govt selling vehicle and DL data of Indians for Rs 3 crore, 87 private companies already bought. *India Today.* 10 July.
https://www.indiatoday.in/auto/latest-auto-news/story/govt-selling-vehicle-and-dl-data-of-indians-for-rs-3-crore-87-private-companies-already-bought-it-1565901-2019-07-10

selling such data. In the light of the concerns raised earlier over the flaws of anonymisation, this further raises privacy concerns for the citizen.

And there are many more concerns with this provision, including from a business perspective. Thus, for example, non-personal data can include intellectual property (IP) rights (such as copyright and trademark), and that would directly impact innovation. However, the Bill does not prescribe the conditions or manner for requesting data from private entities.

Recommendation:

Sections 91(2) and 91(3) should be omitted from the Data Protection Bill 2019.