Personal Data Protection Bill, 2018

Feedback Based on Latest Economic Thinking

By Subhashish Bhadra, Investment Principal at Omidyar Network

I congratulate members of the Justice Srikrishna Committee for a thorough and well-thought data protection bill. I also welcome the feedback period provided by the Ministry. Most of the submissions are likely to focus on legal aspects and rights. However, my submission focuses on what the latest economic thinking tells about building the right incentives to nudge people to make the best use of the system.

This bill is a major step in India's journey towards a data governance framework that protects individual privacy, enhances institutional strength, and promotes innovation. To achieve these aims, the bill should recognise that privacy is important for innovation. Privacy plays a market-building function by creating trust in the ecosystem. Empirical studies in the US have validated this position.

However, the primary purpose of the bill should be to protect individuals from the new risks and harms that a data-based economy has created. After prioritising this objective, the law should optimise for secondary aims such as ease of business and innovation. With this lens, I have a few suggestions to offer on the bill. My suggestions draw on economic research on this topic across different sectors and geographies. I have attached the details of sections that require amendments, and the empirical studies backing those suggestions.

First, the law will need to wade into *moral* issues. It will need to provide guidance on those uses of data that are acceptable and those that are not. Researchers have shown that more information can both benefit and harm individuals, depending on the context. Consequently, Sections 3, 60, 97 and 108 should be amended to enable the Authority to specify impermissible uses of data. In addition, Section 16, which provides broad exemptions for 'purposes related to employment' should be deleted since such a wide exemption can be misused. Several studies show the widespread existence of data-based discrimination in the employment market.

Second, consent needs to be strengthened to make it meaningful. While the bill lays down broad principles under Sections 12 and 18, more needs to be done to make consent work *in practice*. Researchers have found that standardised privacy policies greatly enhance understanding of the specific provisions. Therefore, Section 12 should be modified to require adherence to consent templates that are specified by the Authority under revised Sections 60, 97 and 108.

Third, the transparency provisions need to be bolstered to ensure better adherence. This will also provide data principals and their representatives the information and tools to protect themselves. Section 32 of the bill should be modified to enforce mandatory data breach notifications to affected data principals. Researchers have shown that mandatory data breach notification reduces identity theft and an average victim's loss, while improving firms' security and operational practices. Sections 33 and 35 of the bill should be modified to make data protection impact assessments and data audits publicly available, after

removing any confidential information. Section 30 needs to be modified to require data fiduciaries to provide information about any data breaches on their website. Many researchers have documented negative consequences of poor data security practices on firms' stock prices. Therefore, making the two documents public will create the right incentives for businesses.

Fourth, a qualified 'Right to Erasure' should be introduced. Theoretical economic literature has shown that retaining old, irrelevant information can reduce societal well-being. The current *Right to be Forgotten* is insufficient because it requires the data principal to approach an Adjudication officer. This lengthy process is likely to discourage erasure requests. Therefore, Chapter V needs to be modified accordingly.

Fifth, the bill should recognise the need for contextual regulation, and therefore have a greater role for sectoral regulators. Economists have noted that 'rather than a uniform piece of regulation to address contemporary privacy issues, a nuanced approach – dynamic and individualised to specific markets, contexts and scenarios – may be necessary'. This have been empirically seen in some markets – for example, different kinds of consent mechanisms have had different impact on the genetic testing market in the US. Therefore, sectoral regulators like RBI and TRAI should be empowered with limited legislative powers, whereas the adjudication powers may remain with the Authority. In particular, Sections 22, 23, 28, 30, 33 and 38 of the bill should be modified to create a role for regulators notified by the Authority under a revised Section 60.

There are other useful suggestions that have been discussed in the past two months, including modifying the exemptions for the state and the data localisation mandate. These are important issues that must be engaged with. However, my submission focusses on the five ways in which the bill can strive towards user-centric, evidence-based data regulation.

Detailed Comments

CHAPTER I

Section 3.21. Sub-section (vi) should read "*any discriminatory treatment as specified by the Authority*". More discussion is required on the acceptable forms of discrimination. For example, charging higher insurance premiums for smokers is also a form of discrimination. The norms around discrimination will also evolve. Therefore, the Authority needs to be able to add to the categories of harms and discrimination. Studies have shown different impacts of privacy on discrimination, depending on context:

- *Goldin and Rouse (2000)* find evidence that blind auditions foster impartiality in hiring and increase the probability that women will be hired
- *Bushway (2004)* and *Strahilevitz (2008)* find that when employers are not able to retrieve pertinent information about a job applicant due to privacy regulations, they may become increasingly reliant on statistical discriminatory strategies (eg. ethnicity)
- *Mikians et al. (2013)* find price differences of 10 to 30% for identical products based on the location and characteristics of different online visitors

CHAPTER III

Section 12.2. Should be changed to '*For consent of the data principal to be valid, it must meet the template(s) prescribed the Authority or the relevant regulator. If such a guideline is not available, it must be …*" This is required because economic literature shows that consent is better understood when privacy policies are standardised.

- *Kelley et al. (2010)* find that standardised privacy policy presentations can have significant positive effects on accuracy and speed of information finding and on reader enjoyment of privacy policies.

Section 16. Should be completely deleted. Such a broad exemption for 'purposes related to employment' can be misused. Any data required by the employer should be consented to as part of the employment agreement. This is because several studies show the existence of data-based discrimination in the employment market. Even when such data is not sensitive, it can reveal information that can be used for discrimination. For example, names (non-sensitive) can be used to infer caste and ethnicity (sensitive), resulting in discrimination.

- *Bertrand and Mullainathan (2004)* find that employers may infer candidates' personal traits from information available on their resumés, and use that information to discriminate among prospective employees
- *Acquisti and Fong (2013)* find evidence of both search and discrimination among a self-selected set of employers

Section 17.2. Should not include 'credit scoring'. All data required for such scores can be collected after taking consent. While there has been no direct study on the impact of credit scoring, lower privacy protections have been shown to result in greater denial of credit in the US financial market.

- *Kim and Wagman (2015)* find that opt-in provisions (which are usually better for privacy) resulted in greater approval rates for loans than opt-out provisions

CHAPTER IV

Section 22.1. Should read '*Such further categories of personal data, as may be specified by the Authority or other notified entities, shall be sensitive personal data and, where such categories of personal data have been specific, the Authority or other notified entities may also specify any further grounds on which such specified categories of data may be processed.*' This will introduce sectoral and geographic context into data protection regulation. This is required because studies have found varying impact of privacy provisions on aspects like innovation.

- *Miller and Tucker (2004)* found studied three approaches taken different US states to protect patients' genetic privacy: requiring informed consent, restricting discriminatory usage by empowers, and limiting redisclosure without consent. They found that the three had different effects: while redisclosure encouraged the spread of testing, requiring informed consent deterred it.

Section 22.2. Should read '*The Authority or other notified entities shall specify categories of personal data under sub-section (1) having regard to –"*

Section 22.2. Should read "*The Authority or other notified entities may also specify categories of personal data, which require additional safeguards or restrictions when repeated, continuous or systematic collection for the purposes of profiling take place and, where such categories of personal data have been specified, the Authority or other notified entities may also specify such additional safeguards or restrictions application to such processing."*

CHAPTER V

Section 23.3. Sub-section (d) should read "*such other factors as may be specified by the Authority or other notified entities"*

Section 23.4. Should read "*The Authority or other notified entities shall notify the following as guardian data fiduciaries –"*

Section 23.6. Should read "*Sub-section (5) may apply in such modified form, to data fiduciaries offering counseling or child protection services to a child, as the Authority or other notified entities may specify.*"

CHAPTER VI

New Section: Right to Erasure. Should be added because economic literature demonstrates that retaining old, irrelevant information can lead to improvement in societal outcomes. The existing *Right to be Forgotten* is insufficient because it requires the data principal to approach the Adjudication officer. This will make the exercise of this right more difficult. Therefore, a *Right to Erasure* based on the GDPR right should be considered.

- Blanchette and Johnson (2002) find that there can be social benefits from "forgetfulness"

Section 26.2.c. Should read "*compliance with the request in sub-section (1) would reveal a trade secret of any data fiduciary or would not be technically feasible because it is not held electronically.*" Such a qualification is required to prevent data portability requests from being denied easily. Data portability is seen to improve welfare in the economy.

- *Miller and Tucker (2011)* found that greater data portability through higher adoption of health information exchanges (HIEs) in the US resulted in lower annual deaths of US-born babies

Section 28.3. Should read "*The Authority or other notified entities may specify a reasonable time within which data fiduciary shall comply with the requests under this Chapter, and such time period shall be communicated to the data principal along with the acknowledgement referred to in sub-section (1). In case of a different time period being specified by the Authority and any notified entity, the lesser of the two shall apply*."

CHAPTER VII

Section 29. Should have another sub-clause (h) that reads "*technology and data practices are used in a way to minimise the ability of employees and third parties to cause harm to the data principal."* Studies have found that encryption alone is not enough, and insider attacks are a common source of data breaches.

- *Miller and Tucker (2011)* find that encryption increases the cases of publicised data loss due to internal fraud or loss of computer equipment. Encryption requires careful data management policies to be successful and does not ward off insider threat.

Section 30.1. Should have another sub-clause (h) that reads "*any data breach suffered by the fiduciary that caused harm to any data principal*." This is because information about the data breaches suffered by a company has been shown to reduce its stock price. Therefore, disclosure of such information will create the right incentive for firms.

- *Cavulsoglu et al. (2004)* find that disclosure of a security breach results in the loss of 2.1% of a firm's market valuation over two days.

Section 30.1.h. Should read "*any other information as may be specified by the Authority <u>or other notified entities</u>*."

Section 32.1. Should read "*The data fiduciary shall notify the Authority <u>and affected data principals</u> of any personal data breach relating to any personal data processed by the data fiduciary where such data breach is likely to cause harm to any data principal.*" Studies have shown that mandatory data breach notifications lead to better outcomes for individuals.

- *Romansky et al. (2011)* find that adoption of data-breach disclosure laws reduces the incidence of identity theft by 6.1%
- *Schwartz and Janger (2007)* find that data breach disclosure laws reduce an average victim's loss and improve the firm's security and operational practices

Section 32.5. Should be deleted in response to the modification to Section 32.1 proposed above.

Section 32.6. Should be modified to "*The Authority may direct the data fiduciary to take appropriate remedial action as soon as possible"* in response to the modifications to Sections 30.1 and 32.1 proposed above.

Section 33.2. Should read "*The Authority <u>or other notified entities</u> may, in addition, specify those circumstances, or classes of data fiduciaries, or processing operations where such data protection impact assessment shall be mandatory, and may also specify those instances where a data auditor under this Act shall be engaged by the data fiduciary to undertake a data protection impact assessment."*

Section 33.5. Should have a new sub-section (a), which states that "*All such data impact assessments should be made publicly available on the website of the data fiduciary, after removing any confidential information or trade secrets, in case the processing in question has been undertaken.*" This is because information about the data breaches suffered by a company has been shown to reduce its stock price. Therefore, disclosure of such information will create the right incentive for firms.

- *Campbell et al. (2003)* find that stock prices of firms reduce by 5.4% in response to breaches caused by unauthorised access

Section 35. Should have a new sub-section (8) which states that "*All such data audits should be made publicly available on the website of the data fiduciary, after removing any confidential information or trade secrets*." This is because information about the data breaches suffered by a company has been shown to reduce its stock price. Therefore, disclosure of such information will create the right incentive for firms.

- *Telang and Wattal (2007)* find that software vendors' stock prices suffer when vulnerability information about their products is announced

Section 38.1. Should read "*The Authority or other notified entities shall, having regard to the following factors, notify certain data fiduciaries or classes of data fiduciaries as significant data fiduciaries –"*

Section 38.2. Should read "*The notification of a data fiduciary or classes of data fiduciaries as significant data fiduciaries by the Authority or other notified entities shall under sub-section (1) shall require such data fiduciary or class of data fiduciaries to register with the Authority in such manner as may be specified*."

CHAPTER IX

Section 45.2. Should read "*For the purpose of sub-section (1), the Authority or other notified entities may exempt different categories of research, archiving, or statistical purposes from different provisions of the Act."*

CHAPTER X

Section 60.2. Should have another sub-section (y) stating "*appointing other sectoral regulators as notified entities to undertake activities as defined in Sections 22, 23, 28, 30, 33 and 38."*

Section 60.2. Should have another sub-section (z) stating "*specifying templates for collection of consent under Section 12*."

Section 60.2. Should have another sub-section (aa) stating "*specifying discriminatory treatment under Section 3*."

CHAPTER XI

Section 69.1. Should have a new sub-section (f) stating "*Failure to disclose a data breach to affected data principals*"

Section 69.2. Should have a new sub-section (g) stating "*Failure to provide a data impact assessment to the public in accordance with the provisions of Section 33*"

Section 69.2. Should have a new sub-section (i) stating "*Failure to provide a data audit to the public in accordance with the provisions of Section 35*"

CHAPTER XIV

Section 97.6. Should have a new sub-section (k) stating "*template(s) for collection of consent under Section 12"*

Section 97.6. Should have a new sub-section (k) stating "*specifying discriminatory treatment under Section 3"*

CHAPTER XV

Section 108.2. Should have a new sub-section (ee) stating "*template(s) for collection of consent under Section 12*"

Section 108.2. Should have a new sub-section (ff) stating "*specifying discriminatory treatment under Section 3*"