Legislative Brief

The Personal Data Protection (Draft) Bill, 2018

The Draft Bill was presented to the Ministry of Electronics and Information Technology on July 27, 2018, by the Committee of Experts under the Chairmanship of Justice B. N. Srikrishna.

Recent Briefs:

[The DNA Technology (Use and Application) Regulation Bill, 2018]

November 26, 2018

[The Trafficking of Persons (Prevention, Protection and Rehabilitation) Bill, 2018]

October 30, 2018

Mandira Kala
mandira@prsindia.org

Ahita Paul
ahita@prsindia.org

December 21, 2018

Highlights of the Bill

- The Bill regulates the processing of personal data of individuals (data principals) by government and private entities (data fiduciaries) incorporated in India and abroad. Processing is allowed if the individual gives consent, or in a medical emergency, or by the State for providing benefits.
- The data principal has several rights with respect to their data, such as seeking correction or seeking access to their data which is stored with the fiduciary.
- The fiduciary has certain obligations towards the individual while processing their data, such as notifying them of the nature and purposes of data processing.
- The Bill allows exemptions for certain kinds of data processing, such as processing in the interest of national security, for legal proceedings, or for journalistic purposes.
- The Bill requires that a serving copy of personal data be stored within the territory of India. Certain critical personal data must be stored solely within the country.
- A national-level Data Protection Authority (DPA) is set up under the Bill to supervise and regulate data fiduciaries.

Key Issues and Analysis

- The data fiduciary needs to inform the DPA of a data breach if it is likely to harm the individual. There may be a conflict of interest while assessing whether a breach is to be reported, as the fiduciary is regulated and evaluated by the DPA on several parameters, including instances of data breaches.
- The Bill allows exemptions for purposes such as journalism, research, or legal proceedings. It could be questioned if these meet the standards of necessity and proportionality required for infringements to an individual's right to privacy.
- The State is not required to seek the individual's consent while providing benefits or services. It is unclear why this exemption is not limited only to welfare services of the State, as proposed in the Justice Srikrishna Committee Report.
- The Bill mandates storage of a copy of personal data within India to expedite law enforcement's access to data. This purpose may not be served in some cases, such as when the fiduciary is registered as an entity in a foreign country.
- It could be questioned why the DPA can exercise powers, such as arresting and detaining violators of the law in prison, without approval or order of a court.

PART A: HIGHLIGHTS OF THE BILL[1]

Context

Data protection refers to policies and procedures seeking to minimise intrusion into the privacy of an individual caused by collection and usage of their personal data. In India, usage of personal data or information of citizens is regulated by the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, under Section 43A of the Information Technology Act, 2000.[2] The Rules define personal information of an individual as any information which may be used to identify them. They hold the body corporate (who is using the data) liable for compensating the individual, in case of any negligence in maintaining security standards while dealing with the data.

Over the years, rapid technological advances have led to large volumes of data being generated through various activities, and increasing reliance of businesses on data-driven decision making.[3] Large-scale collection and usage of data by the government for provision of State benefits have also been enabled. One example of this is the biometric identification and verification system of Aadhaar that enables the government to ensure targeted delivery of State benefits, such as LPG subsidies.

In 2012, a petition was filed in the Supreme Court, challenging the constitutional validity of Aadhaar on the grounds that it violated an individual's right to privacy. Following this, in August 2017, a nine-judge bench of the Supreme Court declared privacy as a fundamental right of Indian citizens.[4] The Court ruled that the right to privacy is protected by the Constitution as an intrinsic part of the right to life and personal liberty under Article 21. The Court also observed that 'informational privacy', or the privacy of personal data and facts, is an essential facet of the right to privacy.

Countries around the world have developed comprehensive regulatory frameworks to protect an individual's rights with respect to processing of their information.[3] A Committee of Experts was set up under the Chairmanship of Justice B. N. Srikrishna in July 2017 to (i) examine various issues related to data protection in India, (ii) recommend methods to address them, and (iii) suggest a draft data protection Bill.[5] The draft Bill was presented to the Ministry of Electronics and Information Technology on July 27, 2018. It seeks to protect the autonomy of individuals with respect to their personal data, specify norms of data processing by entities using personal data, and set up a regulatory body to oversee data processing activities.

Key Features

- **Definitions:** The Bill defines (i) 'personal data' as any information which renders an individual identifiable, (ii) data 'processing' as any operation, including collection, manipulation, sharing or storage of data, (iii) 'data principal' as the individual whose personal data is being processed, (iv) 'data fiduciary' as the entity or individual who decides the means and purposes of processing data, and (v) 'data processor' as the entity or individual who processes data on behalf of the fiduciary.
- **Territorial applicability:** The Bill governs the processing of personal data by (i) both government and private entities incorporated in India, and (ii) entities incorporated overseas, if they systematically deal with data principals within the territory of India. The central government may exempt Indian entities exclusively dealing with data principals outside the territory of India by a notification.
- **Grounds for data processing:** The Bill allows data processing by fiduciaries if consent is provided by the individual. However, in certain circumstances, processing of data may be permitted without the consent of the individual. These include (i) any function of Parliament or state legislature, or if required by the State for providing benefits to the individual, (ii) if required under law or for compliance with any court judgement, (iii) to respond to a medical emergency, or a breakdown of public order, (iv) purposes related to employment, such as recruitment, or, (v) for reasonable purposes specified by the Data Protection Authority with regard to activities such as fraud detection, debt recovery, credit scoring, and whistle blowing.
- **Sensitive personal data:** Sensitive personal data is defined in the Bill to include passwords, financial data, biometric and genetic data, caste, religious or political beliefs. The Bill specifies more stringent grounds for processing of sensitive personal data, such as seeking explicit consent of an individual prior to processing.
- **Rights of the data principal:** The Bill sets out certain rights of the data principal whose data is being processed. These include (i) the right to obtain a summary of their personal data held with the data fiduciary, (ii) the right to seek correction of inaccurate, incomplete, or outdated personal data, (iii) the right to have personal data transferred to any other data fiduciary in certain circumstances, and (iv) the right 'to be forgotten', which allows the data principal to restrict or prevent continuing disclosure of their personal data.
- **Obligations of the data fiduciary:** The Bill lays down certain obligations on the data fiduciary who is processing personal data. These include (i) processing personal data in a fair and reasonable manner, (ii) notifying the data principal of the nature and purposes of data collection, and their rights, among others, and (iii) collecting only as much data as is needed for a specified purpose, and storing it no longer than necessary.

- **Exemptions:** The Bill provides exemptions to certain data processing activities. It states that processing of an individual's personal data will not be subject to the obligations specified, and the data principal will not have the rights defined in the Bill, if their personal data is processed for the purposes of (i) national security (pursuant to a law), (ii) prevention, detection, investigation and prosecution of contraventions to a law, (iii) legal proceedings, (iv) personal or domestic purposes, and (v) journalistic purposes.
- The only restrictions on data processing for these purposes are those of (i) processing personal data in a fair and reasonable manner, and (ii) ensuring appropriate security safeguards while processing the data.
- Data processing for research purposes may also be exempted to the extent specified by the Data Protection Authority set up under the Bill. Small entities having turnover of less than twenty lakh rupees, manually processing data of less than one hundred data principals are also exempt from most provisions of the Bill.
- **Data Protection Authority:** The Bill provides for the establishment of a Data Protection Authority (DPA). The DPA is empowered to (i) draft specific regulations for all data fiduciaries across different sectors, (ii) supervise and monitor data fiduciaries, (iii) assess compliance with the Bill and initiate enforcement actions, and (iv) receive, handle and redress complaints from data principals. It shall consist of a chairperson and six members, with knowledge of at least ten years in the field of data protection and information technology.
- The DPA shall have a separate adjudication wing to impose penalties and award compensation. Adjudicating Officers shall be specialists with at least seven years of professional experience in subjects including cyber and constitutional law, and data protection. Orders of the DPA can be appealed to an appellate Tribunal set up by the central government, and appeals from the Tribunal will go to the Supreme Court.
- **Cross-border storage of data:** The Bill states that every fiduciary shall keep a 'serving copy' of all personal data in a server or data centre located in India. The central government may notify certain categories of personal data as exempt from this requirement on grounds of necessity or strategic interests of the State. The central government may also notify certain categories of personal data as 'critical personal data', which may be processed only in servers located in India.
- **Transfer of data outside the country:** Personal data (except sensitive personal data which is 'critical') may be transferred outside India under certain circumstances. These include cases where (i) the central government prescribes that transfers to a particular country are permissible, or (ii) the DPA approves the transfer in a situation of necessity.
- **Offences and penalties:** Under the Bill, the DPA may levy penalties on the fiduciary for various contraventions to the law. These include failure to comply with (i) data processing obligations, (ii) directions issued by the DPA, and (iii) cross-border data storage and transfer requirements. For example, the fiduciary has to notify the DPA of any data breach which is likely to cause harm to the principal. Failure to promptly notify the DPA can attract a penalty of the higher of five crore rupees or two percent of the worldwide turnover of the fiduciary.
- Further, any person who obtains, discloses, transfers, sells or offers to sell personal and sensitive personal data shall be punishable with imprisonment ranging up to five years, or a fine of up to three lakh rupees.

PART B: KEY ISSUES AND ANALYSIS

No guidelines for processing of data in a 'fair and reasonable' manner

Bill: Sections 4, 11(2)

The Bill defines 'data principal' as the individual whose data is being processed. The 'data fiduciary' may be a service provider who collects, stores and uses data in the course of providing such goods and services. While processing the data, the fiduciary is obligated to ensure that data is processed 'in a fair and reasonable manner that respects the privacy of the individual'. Further, the fiduciary has to be able to demonstrate to the Data Protection Authority (DPA) that data has been processed in a fair and reasonable manner. In case of a violation of this provision, the fiduciary is liable to a penalty of four percent of the total worldwide turnover of the fiduciary (subject to a minimum of Rs 15 crore).

While the Bill places this obligation on all data fiduciaries, it does not specify any principles or guidelines for what constitutes a 'fair and reasonable' manner of personal data processing. The absence of guiding principles could allow fairness and reasonability standards to vary across fiduciaries processing similar types of data; and fiduciaries in the same industry may develop and follow different standards. Further, in the absence of any guidelines, it may be unreasonable to expect the fiduciary to demonstrate compliance. Note that non-compliance with this provision may entail a significant monetary penalty.

The Justice Srikrishna Committee Report had suggested that courts of law and regulatory authorities should be allowed to evolve principles of fair and reasonable processing.[5] These standards may vary with technological progress over time, and across different data fiduciaries. [5]

Conflict of interest could arise from optional reporting of data breaches

Bill: Sections 3(21), 3(30), 32(1), 35(2), 35(5)

Data fiduciaries are regulated by the DPA set up under the Bill, which assesses their compliance with the law and initiates appropriate enforcement actions and penalties. The Bill states that the fiduciary shall inform the DPA in the event of a data breach (i.e., an accidental or unauthorised use or disclosure of data) only if such a breach is likely to cause harm to any data principal. The question is whether the fiduciary should have the discretion to determine whether a data breach needs to be reported to the DPA.

Selective reporting of data breaches will avoid the DPA from being burdened with high volume of low-impact data breach reports, and also not make the burden of reporting too onerous on the fiduciary. However, there may be a conflict of interest while determining whether a breach is to be reported, as the fiduciary is regulated by the DPA. Instances of breaches and promptness of notification are assessed in independent data audits ordered by the DPA. Audit results are summarised into a score, which is public, and influences the perception of a fiduciary's trustworthiness. Further, fiduciaries have economic interests in downplaying the risk of data breaches, as there have been instances of breaches negatively affecting stock prices of companies.[6]

Exemptions for certain kinds of data processing could be questioned

Bill: Sections 44, 45, 46, 47, 48

The Bill lays down certain obligations on all data fiduciaries for processing the data principal's information. The fiduciary must provide notice to the principal and take their consent before processing. They may use the data only for specified purposes, and store it with suitable security safeguards for no longer than required. Further, the data principal also has several rights with respect to their data, such as the right to (i) obtain a summary of their personal data held with the fiduciary, and (ii) seek correction of inaccurate, incomplete, or outdated data.

However, the above obligations and safeguards do not apply if data is processed for the purposes of (i) national security, (ii) prevention, investigation and prosecution of violations of a law, (iii) legal proceedings, (iv) personal or domestic purposes, and (v) research and journalistic purposes. The question is whether all exemptions defined in the Bill are warranted.

The Supreme Court, in *Puttaswamy vs UoI*, allowed exceptions to the right to privacy of an individual under certain situations. These include cases where a larger public purpose is satisfied by the infringement of privacy of an individual. Such an exemption must be backed by a law, and must be necessary for and proportionate to achieving the purpose. From this, it appears that an exemption for national security, pursuant to a law, may be justified. However, it is unclear if exemptions for legal proceedings, or for research and journalistic purposes meet the requirements of necessity and proportionality. Note that the Supreme Court, in deciding the constitutionality of Aadhaar, had declared the provision to link Aadhaar numbers with SIM cards as disproportionate, and thereby unconstitutional.[7]

The Bill allows an exemption for the disclosure of personal data for legal proceedings such as (i) enforcing a legal right or claim, (ii) defending any charge, and (iii) obtaining legal advice. It can be questioned whether asking for personal information without a court order becomes permissible per this exemption. Further, it is unclear whether the requirements laid out in *Puttaswamy vs UoI* are met by the exemptions for research and journalistic purposes. The legitimate aims of these exemptions – that is, permitting journalistic freedom or building scope for research – have to be balanced against preserving the right to privacy of data principals.

Processing of data for functions of the State does not require consent

Rationale for not requiring consent for provision of services and benefits by the State is unclear

Bill: Sections 13(2), 19

Under the Bill, data fiduciaries (including the State) cannot process an individual's data without their consent. However, the State may process data without consent for certain functions, such as (i) for provision of services and benefits, and (ii) for issuance of certification, licences and permits. The Justice Srikrishna Committee Report had argued that the validity of consent given by the individual while availing State welfare benefits is questionable, given the imbalance of power between the citizen and the State.[5] Thus, data processing for the provision of any service in the nature of welfare benefits should be allowed without the consent of the individual.

Further, the Report states that only those government bodies which are performing functions directly related to the provision of welfare benefits or regulatory functions should be allowed non-consensual processing of data.[5] While the Report acknowledges that non-consensual processing by government entities for all kinds of public functions may be too wide an exception to consent, the Bill allows non-consensual data processing for all services of the State.[5] For example, this would include public sector banks or public sector telecom companies. Private sector counterparts in such sectors would need to obtain the individual's consent before processing their data.

Functions of the legislature requiring non-consensual processing of data is unclear

Bill: Sections 13(1), 19

The Bill allows for processing of an individual's personal data without their consent if it is necessary for any function of the Parliament or state legislature. It is unclear what functions of the Parliament would necessitate such processing of data without the consent of the individual.

Storage of a copy of data within the territory of India

Bill: Sections 40, 41(1)

The Bill states that every data fiduciary shall keep a 'serving copy' of all personal and sensitive personal data in a server in India. The central government may notify certain categories of personal data as exempt from this requirement on grounds of necessity or strategic interests of the State. Also, the government may notify certain 'critical personal data' which shall be processed only in servers located in India.

The definitions of 'serving copy' and 'critical personal data' are not provided

It is unclear what is meant by a 'serving copy' of data. It could be a live, real time replication of data on a server within India, or it could be a backup at a specified frequency. The specification is needed, as costs, implications and implementation timelines for fiduciaries would vary significantly with the exact nature of a 'serving copy'. Further, it may be argued that the broad criteria for classifying data as 'critical' needs to be specified in the law, as this is necessary for fiduciaries to prepare for the requirement of storing this data solely in India.

Benefits of local storage of a copy of data within the country are unclear

The Justice Srikrishna Committee Report had recognised several benefits of local storage of personal data.[5] It could simplify and accelerate the process of accessing data by law enforcement agencies for investigation. It could help prevent foreign surveillance of Indian citizens; and boost domestic research in artificial intelligence.

However, law enforcement may not necessarily be expedited in some cases where the data fiduciary is registered as an entity in a foreign country. Obligations under Mutual Legal Assistance Treaties (MLATs) will continue to apply, as a conflict of law question could arise with the entity being registered in another country.[5] The Justice Srikrishna Committee Report had noted that the MLAT process is time-consuming, and therefore the objective of expediting law enforcement may not be met by locally storing the data.[5]

Further, some data fiduciaries may be discouraged from investing in India as a market due to additional costs arising from setting up duplicate servers; and hence, consumers may not have the choice of availing services of all data fiduciaries. Additional costs may be passed down to consumers for certain digital services. It may have an adverse impact on smaller data fiduciaries who rely on alternative storage mechanisms that may be cheaper.

Note that as per laws in the European Union, Australia and Canada, storage of a copy of data within the country's territory is not required.[3] Further, Australian and Canadian laws allow the data user (fiduciary) to independently ascertain whether data may be transferred outside the country.[3] The Bill necessitates the involvement of the DPA in making this decision, similar to the European Union.

A complaint may be raised only if there is a possibility of harm

Bill: Section 39(2)

The Bill places several restrictions on the processing of data (such as, collection of only as much data as needed for specified purposes, among others), and also provides certain rights to the data principal to take control of their data. However, the data principal may raise a complaint only if a violation of the provisions of the Bill has caused, or may cause them harm. It could be questioned why the mere violation of the rights of the principal is not enough to raise a complaint. The data principal additionally has to demonstrate and prove that harm has been caused to them by unlawful data processing; and this may place undue burden on the data principal.

Powers and functions of the Data Protection Authority

Enforcement of penalties and compensation orders of the DPA does not require a court order

Bill: Sections 78(1), 78(2)

The Bill allows the DPA to impose penalties on data fiduciaries for violation of provisions of the law. Recovery Officers appointed by the DPA shall have the power to enforce penalties and compensation orders of the DPA. The Officers, per the orders of the DPA, may conduct several enforcement actions against the data fiduciary, including (i) attachment or sale of movable and immovable property, and (ii) arrest and detention in prison.

The Bill does not specify that a court order would be required for the above enforcement actions. Other Acts allow regulators such as the RBI or the IRDA to take actions such as attachment and sale of property and arrest of persons only after the approval of a court. However, following the Securities Laws (Amendment) Act, 2014, the SEBI Act permits the Recovery Officer of the SEBI to take such actions on the orders of the Board.[8]

Creation of an exclusive Data Protection Awareness Fund could lead to conflict of interest

Bill: Sections 77(2), 77(3)

The Bill specifies penalties ranging up to fifteen crore rupees or four percent of the fiduciary's global annual turnover for violation of its provisions. Penalties will be credited to the Data Protection Awareness Fund, and be utilised by the DPA for generating awareness about (i) methods of data anonymisation, and (ii) appropriate responses to data breaches, among others. It is unclear why penalties realised under the Bill will not be credited to the Consolidated Fund of India. Creating a separate Data Protection Awareness Fund to be used solely by the DPA could skew the DPA's incentive to levy higher penalties, and thereby present a conflict of interest while adjudicating disputes and redressing grievances. Acts such as the SEBI Act, 1992 mandate that all sums realised through penalties be credited to the Consolidated Fund of India.[9] However, the PFRDA Act, 2013 establishes

the Subscriber Education and Protection Fund to protect the interests of pension fund subscribers. All penalties realised under the Act are credited to this Fund, and used solely by the PFRDA.[10]

Exercising the 'right to be forgotten' involves adjudication by an officer who may not be competent

Bill: Sections 27(1), 27(2), 68(3)

Under the Bill, the data principal can exercise certain rights, such as (i) the right to obtain a summary of their personal data held with the fiduciary, (ii) the right to seek correction of inaccurate personal data, and (iii) the right 'to be forgotten', which allows the data principal to restrict or prevent continuing disclosure of their data. The exercise of the right to be forgotten requires the data principal to approach the DPA with a written request.

An Adjudicating Officer of the DPA has to determine whether the right to freedom of speech or the right to information of any other citizen could be violated by the exercise of the right to be forgotten by the data principal. Such matters are typically interpreted by courts of law. While one of the eligibility criteria for Adjudicating Officers is knowledge and expertise in constitutional law, the Officer may be an expert in a different field, such as data protection. In such a situation, the Officer may not have the expertise to determine the constitutional question of a possible violation of freedom of speech.

Comparison of the Bill with international data protection and privacy laws

There are several provisions in the Bill that differ from standards of data protection and privacy in laws in the European Union, Australia and Canada. Table 1 outlines some of the provisions which are different.

Table 1: International comparison of data protection and privacy laws

Country	European Union	Australia	Canada	India (proposed Draft Bill)
Coverage of entities	▪ Single law for private and public entities.	▪ Single law for private and public entities.	▪ Separate laws for private entities and federal government institutions.	▪ Single law for private and public entities.
Sensitive personal data	▪ Does not include financial data, passwords.	▪ Does not include financial data, passwords.	▪ Not defined separately; any data may be sensitive based on the context.	▪ Includes financial data, passwords.
Storage and sharing of data across borders				
Local storage of data	▪ Not mandatory.	▪ Not mandatory. ▪ Sector specific mandates, e.g., for health data.	▪ Not mandatory.	▪ Mandatory storage of a copy; critical personal data stored only in the country.
Cross border transfer of data	▪ Permitted if the receiving country has adequate standards of data protection, as assessed by the European Commission.	▪ Permitted if the processing entity has taken steps to ensure that the recipient does not breach country's privacy principles.	▪ Permitted if the processing entity uses contractual or other means to ensure comparable level of protection.	▪ Permitted (for some data) if approved by the regulator or prescribed by the government.
Regulation and enforcement				
Data breach notification	▪ Potentially harmful breach must be reported to the regulator. ▪ Individual may not be informed if processing entity has taken corrective measures, or if it involves disproportionate effort.	▪ Potentially harmful breach must be reported to the regulator and affected individuals.	▪ Potentially harmful breach must be reported to the regulator and affected individuals *(amendment not in force)*.	▪ Potentially harmful breach must be reported to the regulator. ▪ Regulator will determine if the individual will be notified, on the basis of severity or need of an action by the individual.
Criminal penalties	▪ No criminal penalties.	▪ No criminal penalties.	▪ No criminal penalties.	▪ Imprisonment up to five years for certain offences.

Sources: European Union - The General Data Protection Regulation, 2016; Australia - The Privacy Act, 1988; Canada - The Privacy Act, 1985; The Personal Information Protection and Electronic Documents Act, 2000; India - The Personal Data Protection (Draft) Bill, 2018; PRS

1. This Brief has been written on the basis of the Personal Data Protection (Draft) Bill, as presented to the Ministry of Electronics and Information Technology, by the Committee of Experts under the Chairmanship of Justice B. N. Srikrishna, on July 27, 2018.
2. Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.
3. Data protection and privacy statutes in various countries: European Union – The General Data Protection Regulation, 2016; Australia – The Privacy Act, 1988; Canada – The Personal Information Protection and Electronic Documents Act, 2000; The Privacy Act, 1985.
4. Justice K. S. Puttaswamy (Retd.) and Anr. vs Union of India and Ors, W.P. (C) No. 494 of 2012, August 24, 2017.
5. "A Free and Fair Digital Economy", Report of the Committee of Experts under the Chairmanship of Justice B. N. Srikrishna.
6. In September 2017, Equifax stock prices fell by 18% after they announced a data breach affecting 143 million people.
7. Justice K. S. Puttaswamy (Retd.) and Anr. vs Union of India and Ors, W.P. (C) No. 494 of 2012, September 26, 2018.
8. Clause 21, The Securities Laws (Amendment) Act, 2014.
9. Section 15JA, The Securities and Exchange Board of India Act, 1992.
10. Section 29, The Pension Fund Regulatory and Development Authority Act, 2013.