Feedback on Personal Data Protection Bill

Observer Research Foundation

Set up in 1990, Observer Research Foundation (ORF) is a one of Asia's preeminent think tanks that provides non-partisan, independent analyses on matters of security, strategy, foreign policy and global governance. ORF's Cyber Initiative hosts CyFy: the India Conference on Technology, Security and Society. It also convenes Track 1.5 dialogues with the United States, the United Kingdom and the European Union on cyber issues. ORF's research revolves around cross-border data sharing, security of digital payments, encryption and emerging technologies.

Over the past few months, ORF has convened three multistakeholder roundtables specifically aimed at obtaining inputs for the data protection law. These roundtables have engaged a wide range of experts from different disciplinary backgrounds. The issues highlighted below represent what we consider pivotal to the new data protection regime. The opinions expressed here, while encapsulating the conversations at the roundtables, have been curated by ORF, and may not represent the views of any participants in attendance. The list of participants in attendance at these roundtables is available on request.

I. Powers of the Data Protection Authority (DPA)

The Draft Bill envisions the establishment of a DPA for the purposes of enforcement, rule-making, imposing penalties and overall regulation of data protection in India.

a. Search & Seizure

The Draft Bill envisions sweeping powers of search and seizure for the DPA contained in Clause 66 of the Draft Bill. It is the only regulator accorded with such powers of search and seizure emanating from the Code of Criminal Procedure, 1973. The DPA may conduct search operations even when it considers a breach to be "likely".

These powers of search and seizure granted to the DPA are not supported by procedural safeguards necessary to prevent regulatory overreach and misuse that can cause disruption of businesses.

The Competition Act, 2002, which has a similar ambit with extra-territorial jurisdiction, does not empower the Competition Commission to conduct search & seizures directly. The Commission is required to apply to the competent Metropolitan Magistrate to sanction search and seizure. Section 41, Competition Act, therefore, provides a useful and time-tested solution in this respect.

The DPA has also been entrusted with rule-making and approval authority on a wide set of matters within the scope of the data protection architecture. This creates room for subjective considerations and an uncertain regulatory regime. Any change in the law is certain to require substantial consequential changes in network architecture and business models. The data protection framework ought to have the flexibility to adapt to new technologies while maintaining a stable business environment.

For instance, Clause 40(2) empowers the DPA to notify categories of "critical personal data" without providing any guiding principles.

Similar provisions in the Draft Bill make the framework prone to constitutional vulnerability on the ground of excessive delegation. The law in this respect is well settled, there cannot be delegation of legislative authority without any guidance contained in the parent Act itself. [1]

***Recommendation*.**

1. It is recommended that the Draft Bill incorporate provisions for judicial oversight in the exercise of the powers of search and seizure.
2. It is recommended that rule-making powers granted to the DPA be informed by guiding principles enshrined within the Act.

II. Onerous Compliance

Significant data fiduciaries are subject to additional compliance requirements that are set out below. These requirements need to be closely examined in order to avoid imposing an unjustified regulatory burden without any gains in data protection.

a. Data Protection Impact Assessment

Clause 33(4) mandates that Data Protection Impact Assessments ("DPIA") must be undertaken by significant data fiduciaries when new technologies are introduced. These DPIAs thereafter must duly filed with the DPA. This will add another layer of regulatory intrusion and increases the administrative burden of the DPA. This filing requirement increases the compliance burden without meaningfully augmenting data protection.

[1] Kishan Prakash Sharma v. Union of India, (2001) 5 5CC 212, para 18 : AIR 2001 SC 1493.

During an inquiry, the DPA in any case has the power to compel the production of any such DPIA conducted by a delinquent data fiduciary. Under the GDPR, the conduct of DPIA is an element in the determination of liability for breach.[2] A similar approach in this regard would reduce compliance burden without compromising on data protection.

b. Data Audits

One of the most significant elements of the audits mentioned in Clause 35(2)(b) is "effectiveness" of privacy-by-design adopted by a data fiduciary. This involves subjective assessment which is opposed to the fundamental assumption of objectivity in auditing.

Similarly, data trust scores that are to be assigned under Clause 35 (5) and (6) involve wide discretion and there are no practicable objective criteria. This defeats the purpose of having an audit requirement to impose accountability.

The data trust scores in Clause 35(5) and (6) are subjective and uncertain if they are assigned by multiple auditors. This would create an incentive for companies to use auditors who tend to assign higher trust scores. This could seriously imperil the sanctity of the auditing process.

Recommendations:

1. Data audit requirement should be amended to state that an auditor is required to certify the "existence" of privacy-by-design.
2. The Bill should introduce an objective scale upon which trust scores can be assigned.

III. Reasonable Purpose Processing

Clause 17 enumerates when non-consensual processing is considered to be reasonable. The purpose of such a provision is to reduce the focus on consent as the basis of the fiduciary-based

[2] Article 35, GDPR.

regime. The purposes incorporated include interests such as credit scoring, fraud prevention and recovery of debt. The foundational basis for this ground of processing is a reasonable expectation of the data principal and the public interest. A similar provision of "legitimate interest processing" has been included in the GDPR.[3] The present proposal, however, varies with the GDPR since the DPA is required to further specify particular reasonable purposes in line with the grounds mentioned. This makes the ground for reasonable processing needlessly restrictive. Data fiduciaries would require greater latitude in this respect in order to meaningfully reduce the involvement of consent for beneficial processing. This acquires importance in view of a specific finding regarding the challenge of consent fatigue in the Report.

Similarly, Clause 45 provides for processing of personal data for research purposes subject to exemption by the DPA. This again adds to the administrative burden of the DPA and creates uncertainty for those businesses that could contribute by investing in valuable research.

Sensitive personal data has been excluded entirely from reasonable purpose processing. The definition in Clause 3(35) includes wide-ranging information such as all financial data. The government should consider permitting reasonable purpose processing for sensitive personal data in certain circumstances for policy goals such as fraud prevention.

Recommendation: The role of the DPA under Clause 17(2) should be limited to providing guidance and clarity with respect to the grounds identified under Clause 17(1) so as to aid beneficial data processing.

IV. Definitions

a. Significant Harm

[3] Recital 47, GDPR.

Clause 3(37) defines significant harm as harm that has an aggravating effect. Harm is defined to include various types of personal injuries that may result from a breach of any obligations under the proposed framework.[4] Significant harm is an important element of the criminal offence of obtaining, transferring or selling personal data in violation of the framework which could result in an imprisonment of three years.

This usage of significant harm is ambiguous and its use for determination of criminal penalties renders the entire provision constitutionally vulnerable in view of the holding in *Shreya Singhal v. Union of India*[5]. In *Shreya Singhal*, the Supreme Court held that a penal law may not contain any vague or arbitrary elements leaving the constitution of the offence uncertain.

Recommendation: The definition of significant harm should be clarified and specifically defined at least for the purposes of criminal sanctions proposed.

b. Biometric Data

The definition of Biometric Data contained in Clause 3(8) includes all "facial images". This definition is over-inclusive relative to the GDPR and under existing Indian law. The position under existing Indian law[6] and the GDPR[7] is limited to characteristics derived from facial images.

Recommendation: The definition in the Draft Bill should be amended to include only characteristics derived from facial images.

c. Critical Personal Data

[4] Clause 2 (21) Draft Bill.
[5] (2015) 5 SCC 1.
[6] Rule 2(b) Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal data or Information) Rules, 2011
[7] Article 4 (14), GDPR.

The Bill despite envisioning additional and onerous data processing requirements for critical personal data, fails to define what critical personal data entails. This creates ambiguity in the business environment. A legal mandate for local storage and processing of data should be accompanied by clear and exhaustive indication of the kind of data the mandate applies to.

Recommendation: The bill should include a clear and exhaustive definition of critical personal data.

V. Operational and Economic Risks of Data Localisation

Requirements to segregate certain kinds of data and store data in India either completely or in the form of mirror servers will be a burdensome and prohibitive barrier to companies especially SMEs. Such data localisation regimes can be antithetical to the goals of Digital India and Invest India programmes by impeding innovation, hindering ease of business and undermining security.

Studies have shown that data localisation has resulted in significant negative consequences in a given country. The European Centre for International Political Economy (ECIPE) study found that if India introduced economy-wide data localisation, the negative effect on GDP will amount to a negative 0.8 percent, investments will drop by 1.9 percent and would cost the worker almost 11 percent of one average month's salary.[8]

Requirements for local servers will also disproportionately impact small and medium enterprises (SMEs) and the local industry who will be forced to seek out more expensive and less secure services. Localisation can be counterproductive. Instead of creating jobs, these rules will be add to cost of the local businesses.

[8] Bauer et al., The Costs of Data Localisation: Firendly Fire on Economic Recovery, ECIPE Occaisional Paper No. 3/2014, available at: http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf.

As the Report accompanying the draft Personal Data Protection Bill, 2018 acknowledged, even after localisation, law enforcement access to data will likely be impeded by conflict of law. Instead, as the Report noted moving towards harmonising regimes through bilateral agreements will be key.

Operationally, it will be difficult for companies to identify the nationalities of the data owners' when processing any service online. This can be particularly challenging and onerous for companies that would be identified as collecting "critical personal data" under the Bill.

Further, if foreign companies are unable to store data (even through mirroring) in India, users in the country could potentially lose out on access to several parts of the internet – effectively creating a "splinternet".

Additionally, the Report does not effectively address how mandatory data localisation is best suited (or the only viable solution) to meet India's stated interests in improving enforcement of laws, avoiding vulnerabilities of relying on fiber optic network, building an AI ecosystem and preventing foreign surveillance.

Recommendation: Data localisation is an inefficient solution that is not investment friendly and for the benefit of India's digital ecosystem, a localisation mandate should only be used as a measure of last resort.

VI. Access to data based on user location instead of data location for law enforcement

The Srikrishna Committee (Committee) in the Report accompanying the Bill notes that law enforcement access to data for investigation and prosecution of crimes is one of the primary reasons behind requiring data fiduciaries to store data locally. The Committee, however, acknowledges that companies may not comply even with a localisation mandate as conflict in laws might prevent them from doing so. Specifically, the Committee recognizes that national

blocking statutes as found under US law can effectively bar service providers from disclosing user data to foreign law enforcement authorities.[9]

The Committee proposes that states must instead " strive towards harmonisation to create an enforcement regime that provides for effective information sharing."[10]

Access to user data can be based on the jurisdiction of data location, user location or company headquarters' location – in practice, often data, users and companies are situated in different countries. Currently, popular communication service providers adopt the laws of the jurisdiction where the headquarters is located when responding to data requests resulting in countries going through the MLAT and US legal process. This leaves other countries with limited recourse to enforce their domestic laws on citizens within their own territories on issues such as data protection, intellectual property, or criminal law.[11]

The Bill by imposing mandatory localisation has effectively determined that access to data will be governed by the laws of the jurisdiction where the data is stored. Besides the fact that companies may potentially refuse to cooperate citing conflict of laws seeing as the Bill after all requires collectors of personal data to only store a serving copy or mirror servers in India, there are other significant challenges posed by this approach.

First, with companies storing electronic communications in the cloud, data is often broken into "shards" and distributed across different countries. Therefore, companies will be forced to fundamentally alter the architecture of how they operate to adhere to a data localisation mandate. Second, through reading of Clauses 2(1)(a), (b) and 2(2) of the Bill, the application of the act is only extended to processing of personal data by data fiduciaries including the state, any

---

[9] Bedavyasa Mohanty and Madhulika Srikumar, "Data localisation is no solution," (August 2018) *available at* https://www.orfonline.org/research/42990-data-localisation-is-no-solution/

[10] Srikrishna committee report

[11] Kate Westmoreland, "Jurisdiction over user data - what is the ideal solution to a very real world problem?" (July 2014), *available at*, http://cyberlaw.stanford.edu/blog/2014/07/jurisdiction-over-user-data-what-ideal-solution-very-real-world-problem

Indian company or body created under Indian law, any Indian citizen or fiduciaries located abroad that offers goods or services in India or holds a connection with any business in India. The clauses therefore suggest data fiduciaries will be compelled to store date either of Indian citizens or emanating from Indian territory, locally. Data localisation therefore at best can only provide law enforcement access to data for crimes that have been committed in India, where both the perpetrator and victim are situated in India. In cases of transnational crimes such as online radicalisation, cybercrimes, money laundering and sex trafficking, individuals and accounts that are not either Indian or emanating from India will be implicated. As long as access to data is governed by the laws of where the data is stored, Indian law enforcement will lose crucial access to data for investigation in these cases. For investigations into such crimes, Indian law enforcement will have to continue relying on cross-border inter-government mechanisms like the MLAT process.

Moving towards a regime where data access is dictated by the laws of the country where is the user is located would not only ensure that principles of territoriality and sovereignty under international law are met but also enable governments to enforce laws regardless of where the data is stored. In effect, under this framework, Indian users would be protected by the domestic data protection law and legacy statutes which would ultimately determine how governments can access data for criminal investigations. Jurisdiction based on user-location will facilitate Indian law enforcement to access data pertaining to an Indian crime under Indian laws directly from foreign service providers. The US CLOUD Act and Europe's E-evidence rules indicate the trend of governments transitioning towards this regime where local laws determine legitimate access to data for criminal investigations removing any conflict of laws. In this framework, requests can be made by foreign law enforcement or government to the data fiduciaries/service providers directly under domestic laws while ensuring robust protection of privacy and due process. Since this development (once enforced) can repose significant discretion in the hands of companies, clear rules outlining transparency, accountability including challenges by governments and companies to orders for data request have been established.

Recommendation:

1. To bring about a uniform enforcement regime respecting principles of sovereignty, the criteria for government or LEA access to data should be based on where the user is located and not where the data is stored. Therefore, developing a common framework easing conflict of laws and increasing cooperation between states, is essential to discourage further fragmented legal frameworks.
2. The Ministry should explore bilateral data sharing agreements, for example, under the US CLOUD Act that can better serve law enforcement need for data. These agreements should instil robust protections for user privacy and due process.

VII. Anonymisation

Clause 92 of the Bill criminalises re-identification and processing of personal data that has been de-identified by a data processor or fiduciary without the consent of such fiduciary or processor or the principal whose data has been de-identified.

De-identification or anonymisation of data is a strong privacy-protecting principle, but it is not fool proof. Data often considered completely anonymised by the data collector can be re-identified by corelating it with external data sets. In 2007, part of an anonymised data set of movie reviews by 500,000 users published by Netflix was de-anonymised by researchers who compared the reviews with rankings and timestamps publicly available on the Internet Movie Database.

The provision in its current form, is problematic because it deters legitimate cyber security research into anonymised datasets. The present requirement of obtaining consent of either the data fiduciary/processor or data principal prior to re-identification is unrealistic for two reasons. *First*, a data fiduciary/processor that has released an anonymised dataset into the public domain is unlikely to consent to attempts at penetration testing of its anonymisation techniques. *Second*,

for large datasets, the publication of which can lead to violation of privacy of a significant number of individuals, it is impossible to collect explicit consent of each individual.

Recommendation: The clause should be de-criminalise re-identification of anonymised datasets if the person re-identifying the data:

a) re-identifies personal data for research into the strength of anonymisation process or for any other legitimate public interest
b) does not publish the re-identified data in the public domain
c) does not obtain or solicit any commercial gain from the re-identification of the data
d) discloses the findings to the data protection authority within 72 hours, if the dataset or part of the dataset has been successfully re-identified

VIII. Surveillance Reform

The Personal Data Protection Bill's silence on surveillance reform is worrying at a time when pervasive technologies pose a significant harm to data privacy. India's surveillance laws were drafted at a time when mass/bulk surveillance was decades away from being technologically possible. The necessary safeguards against arbitrary and untargeted electronic surveillance were therefore not built into Indian laws.

The Supreme Court in the Puttaswamy judgement, in addition to carving out exceptions such as national security for which data can be collected also laid down tests against which data collection and surveillance practices can be judged. The majority opinion of the court laid down that suspension of an individual's privacy can be done pursuant only to a law drafted by parliament, in furtherance of a legitimate aim, in a manner that is proportionate and supported by procedural guarantees. The requirement for proportionality has also been reflected in Clause 43 of the Bill.

Some Indian laws on electronic surveillance fall afoul of the Puttaswamy test on proportionality and therefore are liable to be revised under the new data protection law. Rule 3(4) of the Information Technology (Procedure and safeguards for monitoring and collecting traffic data or Information) rules, 2009 and Rule 9 of the Information Technology (Procedure ad safeguards for Interception, Monitoring and Decryption of Interception) Rules, 2009 for instance allow the interception of information relating to any "class of persons" or "subject matter."

In effect, provisions such as these allow the use of surveillance technologies that are non-targeted and can invade upon the privacy of entire sections of the population at the same time. This is clearly contrary to the national security exception for the right to privacy which must be proportionate.

Access to data for law enforcement currently takes place through a legacy law in the form of Section 91 of the Code of Criminal Procedure. For instance, to obtain non- content data from foreign companies and any data from Indian companies an investigating officer only produces a notice with no legally recognised format. This process not only lacks safeguards but also makes no distinction between sensitive and non-sensitive data. Given these realities, the data protection Bill should consider a complete overhaul of access to data, specifying different legal treatment for more sensitive data sets. Until such time, calls for data localisation may be premature.

Recommendation:

1. The Ministry should undertake an assessment of all legacy laws that allow access to data in a disproportionate manner and supplement these laws with a judicial oversight mechanism.
2. The Ministry should also take this opportunity to revisit current policies like Clause 39.1 of the Unified License Service Agreement and Part 1, Clause 2.2(vii) of the Internet Service Provider License that impose restrictions on bulk encryption and can have the effect of nullifying strong data privacy principles.