RECOMMENDATIONS BY THE CYBER PEACE FOUNDATION ON
THE PERSONAL DATA PROTECTION DRAFT BILL, 2018.
Recommendation 1:

Applicability of the Act:

- It is recommended that Section 2(3) be omitted altogether. In this evolving digital economy, the types and vectors of attacks are also growing. In many publications, it is now being highlighted how the possibilities of de-anonymization attacks are growing. In the years to come, it is possible that it becomes a common reality which is when we should be ready in terms protecting through law. In our opinion, the approach taken by Singapore is fitting for a situation of the future. A related amendment in the definition of personal data will suit the need. It is recommended that all data that can identify a user should be called personal data which would cover also pseudo or anonymized data sets leaving no scope of vague interpretation by data fiduciaries.

- Under Section 2(2)(a), considering a situation- a blog type of website, that is not ideally offering any goods or services but instead is just getting users to read news or some other content. Whether incorporated outside the country or perhaps not incorporated at all, would such a blog fall under the ambit of this Act. It is relevant because a lot of cookies are generated about users through these blogs and users are often profiled for their behavior and interests etc. All of this amounts to personal data which needs protection. Jurisdiction should be extended in such a way that the DPA/Courts should be given the power to decide on jurisdiction like in the Banyan Tree Case where the level of passiveness of a website definitely does play a crucial role.

Recommendation 2:

Definitions:

- Section 3(3) be omitted in lieu of a better definition of personal data itself.

- Personal data definition under 3(29) be changed to “any data about an individual which in itself or in conjunction with other information that the data fiduciary may have access to, may identify an individual”- Such a definition will cover even pseudo or anonymized data which might lead to identification of people through certain means or attacks. Sometimes, anonymization may be undertaken for the mere purpose of let us say cross-border data flows, sharing or dealing in data etc. What happens in such a scenario when the data fiduciary has access to other data sets that can be used to de-anonymize this data set is a question that the bill is not in a position to answer.

---

The definition of processing has been copied verbatim from the GDPR which is fine but the related definition of profiling has not been which is quite restrictive in our opinion. Ideally, the definition of profiling under 3(33) should be amended to include “calculate, assess any characteristic of a data principal or his life.”

**Recommendation 3:**

**Data Protection Obligations:**

- Purpose limitation under Section 5(2) lays down a test of reasonable expectation. While in law, reasonable expectation doctrine is a development of the English law pointing to the situation where in a contract, interpretation of any provision has to be done as per how a reasonable person (who is not ideally tech or law savvy) would expect it to be. In this space of data privacy, what a reasonable expectation would be is a judicial question that has not been answered yet. In a practical implementation scenario, this will create ambiguity. Till a judicial body rules on the subject, fiduciaries and processors will exploit the provision to use principals’ data for incidental purposes which they might not obtain consent of the principal for.

- Under Section 8, the notice should specifically contain whether data of the principal will or will not be used for profiling. It is a concern that many principals have but do not usually know how to look for in a notice.

- Under Section 10, when a data processor retains data for the fiduciary, there is no specification as to whether there is some difference in time duration of holding data by both the parties. Again, reasonable necessity is something which should a catch all clause. In all situations otherwise, it should be mandated that the time duration of holding data should be specified in the notice. A blanket provision of reasonable necessity will only create problems. A simple example could be holding of data for law enforcement use. Like now a social media company in the US retains data for 90 days for law enforcement use, either we should have a specification of the similar nature for all different types of retention or there should be a mandate to specify in the notice itself.

**Recommendation 4:**

**Grounds for Processing of Personal Data:**

- Under Section 12(5), where the burden of consequences for withdrawal of consent is placed on the data principal, a requirement of notice to be given to the data principal should be added. Something like- once a data principal withdraws consent from a service and there can be consequences in terms of costs or damages, the fiduciary should give a notice that withdrawal of such consent will lead to consequences enumerated. This is done to protect the consumer. An end user today is not well versed with the concepts of privacy and consent and education about privacy is absent from the Indian ecosystem. In order to protect his rights, such a provision is needed.
• Because processing of data includes disclosure, dissemination, indexing etc., the power vested for processing data of an individual for functions of the state can lead to unexpected situations. There should be a catch clause within Section 13 that states “such processing should be undertaken only if the fiduciary is vested with the exclusive authority under a law to process such data.”

• Section 16 of the Bill should be edited to remove all cases of employment and instead be made specific to “performance of any contract that the principal is a party to.” Another fetter to be added in the section is “while processing of data, if the fiduciary makes any disclosure of data to any third party, the data principal must be given information of such disclosure.”

• Under Section 17, the reasonable purposes is a needed provision. However, with the help of schedules, there should be different notifications for acceptable reasonable purposes to avoid any ambiguity.

**Recommendation 5:**

**Data Principal Rights**

• Right to withdraw consent is not an actionable right under this chapter or the bill. It should be clearly specified in the chapter on rights for academic and practical implementation purposes.

• Under Section 27, the data principal should have a right to data erasure along with the right to be forgotten. As a Civil Society body, we have seen multiple cases where certain data about an individual leads to illicit use and there is no provision in any law for content takedown. A specific right to data erasure at least in cases where obscenity is involved except for public interest should be added. This right should be available against data fiduciaries and appealable further.

**Recommendation 6:**

**Transparency and Accountability Measures**

• Breach Notification under Section 32 is not well founded. The decision as to whether there would be any harm to the principal is left to be taken by the fiduciary. Practically, the fiduciary might not notify the DPA at all. In addition, the provision to notify breaches should be made for the data principals. The likeliness clause should be removed.

• The breach notification disclosure timeline is not specified which can be misused by companies to save the image. The onus of declaring a breach to a principles lies with the Data Protection Authority, so the right to information of personal data falls in jeopardy to certain extent, as the Authority may not have right information or parameters to declare about a breach and the data principles might get left with no viable justification, if they come to know externally, which can be a possible case in world of penetrative media.
Recommendation 7:
Transfer of Personal Data outside India-

While one serving copy provision under Section 40 of the Bill is a welcome step in terms of access to data for law enforcement and national security agendas, it is not going to solve the problem associated with data storage outside the country. World over, the adequacy test has been recognized to be the best possible. India should adopt the same strategy as well.

But as a civil society body, we also realize the problems that both state interests and industry interests would face. As for critical data and sensitive data that may be notified via schedules and rules, heightened requirements of data localization need to be enforced with total ban on cross border flow. As for all other data, either there should be adequacy tests or bi-lateral treaties with countries for agreeing on data security and quality requirements etc.

Recommendation 8:
Powers of the Data Protection Authority -

For powers of DPA given under Section 62-66, the persons authorized by the authority must have techno legal background to ensure that the maximum level of efficiency and that legal compliance is achieved.

Recommendation 9:
Notice -

- Digital literacy in India is not at par with developed countries hence u/s 8(2) shall also include a situation is illiterate and unable to understand the written material.

- Color coded scheme can be implemented to signify the level of severity involved in processing of data.

- The purpose of data collection whether the data is manually processed or is processed automatically should be mentioned in notice.

- Whether the data collected after giving consent be used for profiling should be clearly mentioned in clause 1 of Sec 8.

Recommendation 10:
Data Principal Rights

- Right to be forgotten given u/s 27 has a limited scope and enforcing this right doesn’t result in deletion of data, it only restricts or prevents disclosure of the data for the purpose of processing. The scope of this right must be widened to include the right to erasure so that the Indian data protection is at par with GDPR and PDPA Singapore.
The general procedure given u/s 28 for exercising of right given under chapter VI specifies making a request to the data fiduciary for exercising a particular right. However, right to be forgotten u/s 27 specifies making a application to the Adjudicating Officer (AO). Even for the enforcement of this right a reasonable time needs to be given to the data fiduciary for erasure/deletion/removal of personal data of a data principal in order uphold the principles of natural justice. In practical application, it will be tedious task for the data principal attend hearings at the AOs office after initiating quasi-judicial proceeding without giving them reasonable opportunity for erasure/deletion/removal of the data.

- Though, withdrawal of consent is mentioned in Sec 8(1)(d) and 12(2)(e) it must be recognized as a separate right under this chapter so that it can be enforced as per the conditions given u/s 28.

**Recommendation 11:**

Data Protection Authority -

When a nation wants to implement an all sweeping law like the Personal Data Protection Law, a nodal agency appointment is mandatory. The Law establishes the office such an Authority to enforce the bill. Along with enforcement, the law mandates the DPAI to promote awareness, conduct audits, enquiries and issue code of conduct for data fiduciaries. The bill also gives the power to define many parameters and conditions how data fiduciaries and data principles will interact in the new data regime in the country.

Prima facie the powers bestowed on this body are very wide. The principles to govern the transactions or take decisions under this law are not clearly defined and to an extent left to the Authority to define, which may lead to multiple cases of conflict and ambiguity in code of practices. The search and seizure rights of the Authority are discretionary and may lead to stalled businesses. Similarly, the selection committee should have more experts from Cyber Law, Governance Risk & Compliance, Data Security, etc domain to augment the capacity and brings in core technology expertise to complement the law expertise which the Supreme Court Judge and the Cabinet Secretary would bring in.

About Cyber Peace Foundation - Cyber Peace Foundation (CPF) is an award winning international think tank working towards the goal of fostering cyber peace and safety across the internet beneficiary system with focus on cyber security and policy advocacy. Areas of CPF’s work are Technology Governance, Policy Review, Advocacy, Capacity Building, Research and Development.
Recommendation 12: Right to be Forgotten u/s 27

Issue 1: Scope of the Right

The scope of the right given under Section 27 of the bill is limited only to restriction or prevention of a disclosure of a data principal’s data by a data fiduciary. This right can be availed when such disclosure has –

- Either served the purpose or it is no longer necessary
- Consent given under Section 12 has been withdrawn
- Disclosure made in the contravention of existing laws

In addition, clause (2) of Section 27 states that for availing this right, it must override the right to freedom of speech and expression and the right to information of any citizen.

Prima facie, the scope under this section does not cover the deletion or erasure of a data principal’s data stored by a data fiduciary. Comparing this right with similar rights given under various national and international regimes, the scope of this right must be widened. Though this right has gained prominence only in the last decade or so, it is equated with the Right to Erasure.

As per Article 17 (Right to Erasure – ‘right to be forgotten’) of GDPR, the grounds for availing this right are more or less same, but the extent is not. Article 17 of GDPR states that a data subject has a right to erasure of personal data concerning him or her without undue delay and the controller has an obligation to erase the personal data of a data subject on the basis of mentioned grounds. Similarly, The UK DPA 2018 has recognized the same right under its Schedule 6.

The question of whether an individual has a right to be forgotten which includes erasure of data has been brought up before the Indian Courts as well. Such courts include the High Courts of Gujarat, Delhi, and Karnataka. In February 2017, the Karnataka High Court recognised the right to be forgotten for removal of the petitioner’s name from various case reports publicly available results via search engines. According to the Justice Anand Byrareddy who presided over this case, this right can be availed in cases involving women in general and highly sensitive cases involving rape or affecting the modesty and reputation of the person concerned.

Since the bill recognises various rights of data principals with respect to their data and privacy, the right given under Section 27 shall also incorporate the right to erasure/deletion of data.

Possible Solutions:

1. Appropriate modifications can be made in the present Section 27 of the bill by including words such as deletion and erasure. Along with this, additional grounds or restrictions can be added under Section 27(1) for availing this right.

2. An altogether different section can be added under Chapter VI of the bill for erasure or deletion of data. This section should cover situations where personal videos of victims are uploaded on online platforms without their consent, e. revenge pornography cases. Misuse of such a right can be prevented by narrowing the scope of the right using the Balancing principle, as discussed in Chapter 5 of the report.
3. Right to erasure can also work as a right to be deidentified from the information stored with a data fiduciary.

“Deidentification” has been defined by Section 18 of Australia’s ACT IPA 2014 which is on the similar lines as the definition of “anonymisation” given under Section 3(2) of the bill.

Issue 2 – Procedure for Exercising the Right

As per clause (4) of Section 27, a data principle can exercise his or her right to be forgotten by filing an application with the Adjudicating Officer. For the other rights given under Chapter VI of the bill, Section 28 lays down the procedure for exercising those rights by making a request in writing to the concerned data fiduciary. This procedure for exercising the right to be forgotten by stating that the data fiduciaries will be burdened with content removal requests and their decision will be biased towards their own interests. Further, the Committee stated that a data fiduciary is not capable of deciding between the statutory right to be forgotten and the fundamental rights to free speech and information.

Taking into consideration that an Adjudicating Officer (AO) is designated for each state at its capital, the pendency of cases can very well be inferred from the existing judicial system. On the other hand, India has a number of states covering vast geographical areas. For a data principal to appear at each hearing on his application, travelling costs and other practical factors may demotivate a data principal and result in losing the trust in the legal setup prescribed by the bill.

Or for a body corporate having its registered office in Mumbai, the same factors will come into play if they are called to appear before any Adjudicating Officer of the north-eastern states.

Possible Solutions

1. Just like other rights given under Chapter VI of the bill, the data fiduciaries shall be given an opportunity to erase or delete the data of a data principal. If the interests of a data principal supersede the interests of a data fiduciary in continuing to store it, the data must be deleted. For restrictions on the right to erasure, Recitals 65, 66, and 73 of the GDPR along with Section 35 & 36 of Malaysian PDPA 2010 can be referred to.

2. A statutory time limit of up to 30 days must be prescribed for dealing with such a request. A similar time-limit of 36 hours has also been prescribed under Rule 3(4) of the Information Technology (Intermediaries Guidelines) Rules, 2011.

3. If a request for erasure or deletion of data is received or an order from an Adjudicating Officer has been received regarding the same, it must be the duty of a data fiduciary to inform all other data fiduciaries/processors with whom the data was shared. This duty has been recognised by Section 48 of UK DPA 2018 which further adds an obligation to inform all the recipients e. all the parties with whom data fiduciary had shared the data to erase it. A similar obligation has also been enforced under sub-clause (b) of Section 22(2) of the Singapore PDPA 2012.

4. If a data principal is not satisfied with the response given by a data fiduciary, he can follow the standard procedure of filing an application with the Adjudicating Officer.
Recommendation 13: Exemptions under the Bill

Issue 3 – No Exemption to the Armed Forces

Under Chapter IX, the bill grants exemptions to certain purposes which are laid down from Section 42 to 48. These exemptions include processing of personal data for –

- Security of the state
- Prevention, detection, investigation, and processing of contraventions of law
- Processing for legal proceedings
- Research, archiving or statistical purposes
- Personal or domestic purposes
- Journalistic purposes
- Manual processing by small entities

After going through various legislation enacted by the countries across the world, one can arrive at a conclusion that the armed forces of a country must be given a specific exemption under a data protection framework as the processes and procedures of the Armed Forces are altogether different from the procedure established by the law of the land for civil and criminal courts.

Section 70 of APA 1988, Section 7(3)(c.1) under Division I of PIPEDA, 2000, Section 23 of NZPA 1993, and Clause 7 Schedule 11 of UK DPA 2018 are some of the provisions of legislation across the world where Armed/Defense forces have been granted exemption from the national data protection framework in some way or the other.

Possible Solutions

1. A separate section under Chapter IX can be added for granting an exemption to Armed Forces, as done by the legislation mentioned above.

2. The exemption given under Section 42 of the bill i.e. Security of the State can be defined under Section 2 to include armed forces. For this definition, the definition of the phrase national interest given under Section 2 of Singapore PDPA, 2012 can be referred to. This phrase has been defined as

“national interest includes national defence, national security, public security, the maintenance of essential services and the conduct of international affairs.”

Recommendation 14: Offences under the Bill

Issue 4 – Bailable & Non-bailable

Chapter XIII in the bill lays down various offences related to personal data of a data principal. This chapter also contains provisions when offences are done by either companies or Central/State government departments. After around 18 years of the enactment of the Information Technology Act, 2000, we have not been able to realize its potential due to non-consideration of the sensitivity of the harm involved while classifying an offence as bailable and non-bailable. Here in the same chapter, Section 93 specifies that the offences defined in this act are cognizable and non-bailable without considering the sensitivity of the data.
Possible Solution

Whether an offence should be bailable or not should depend on the nature of the data affected. For offences involving sensitive personal data, the offences shall remain non-bailable while for the offences involving disclosure of personal data, the offences should be bailable.

Issue 5 – Power to Investigate

Another reason for non-realization of full potential of the Information Technology Act, 2000 is the power of investigation resting with a police officer, not below the rank of Inspector. The same status quo has been incorporated in the bill under Section 94. This section may be efficiently applicable in urban areas, while the same statement might not hold true for the police stations in suburban or rural areas as they are often headed by a police officer having the rank of Sub-Inspector. In addition, there is generally one police officer per police station having the rank of Inspector who is also designated as the station incharge while there are at least 2-3 subordinate officers having the rank of sub-inspector.

Possible Solution

The power to investigate for the offences given under the bill shall be given to a police officer, not below the rank of a sub-inspector.

Recommendation 15: Power and Functions of Authority

Issue 6 – Blanket Powers of DPA

Section 60 & 61 under Chapter X of the bill discusses various powers, functions, and responsibilities along with a prescription of standard Codes of Practice by the Data Protection Authority (DPA). These powers are given with respect to definitions of processing given u/s 3(32), data fiduciary given u/s 3(13), and data principal u/s 3(14). The provisions given under these sections give a blanket power to DPA to regulate the relationship between a data principal and data fiduciary.

As per the definition of data fiduciary, it can be any person including the State, a company, or any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data. This impliedly means that the number of data fiduciaries in the Indian cyber space will be substantially high. In order to balance between the interests of data principals as well as data fiduciaries, an independent board shall be set up to prescribe technical standards for activities defined under the definition of processing u/s 3(32).

Possible Solution

An independent board such as the Banking Codes and Standards Board of India (BCSBI) can be set up to lay down the technical standards for various processing activities defined under Section 3(32). The power given to DPA can be limited to enforcement of these standards and suggest appropriate changes to these standards to the said board. This board shall comprise of technical as well as legal experts having domain-specific knowledge in the activities given u/s 3(32).
Miscellaneous Recommendations and Suggestions

- The scope of the act given under Section 2 shall also include the data collected offline but processed or stored online.

- This bill is also silent on the aspect of ownership of personal data of a data principal. The bill must recognize data principal as the owner of his or her personal data.

- With possible technological advancements, it is possible that re-identification of a data principal is possible even after anonymisation of his data and hence, processing of anonymised data shall also be brought under the scope of this act by making changes in the definition of personal data.

- The definition of personal data u/s Section 2(29) does not specify whether it covers false information as well. Definition of personal data u/s 2 of Singapore PDPA, 2012 includes data about an individual whether true or not and hence, on the similar lines, the phrase whether true or not can be added to the definition in the bill.

- If a data principal exercises his rights given under Chapter VI, the concerned data fiduciaries shall also inform other fiduciaries with whom the data was shared.

- The notice framework given under Section 8 of the bill shall also include information such as –
  1. Whether data will be manually processed or automatically
  2. Whether the collected data will be used for profiling or not
  3. Whether the collected data will be used for direct marketing or not

- Majority of the debate on data protection in India is based on various reported incidents related to Aadhaar. Hence, UIDAI shall also be brought under the scope of this bill as a data fiduciary and power to enforce the provisions of the bill, as well as the remedies, shall be left to DPA and its adjudication wing.

- The definition of harm under Section 2(31) shall also include non-physical harms.

- Section 10 of the bill talks about limiting the storage limitation on the personal data of a data principal. In many cases, a data fiduciary may consider reasonably necessary duration to an extent which is highly beneficial in its favour. To prevent this, the duration for which personal data will be stored can be specifically mentioned in the notice under Section 8, subject to legal or regulatory requirements.

- For notification of a data fiduciary as a guardian data fiduciary, certain certification requirements must be prescribed and public opinion must be sought on this notification in order to cross-check the image of the said data fiduciary.

- Although the right to withdraw consent has been mentioned in the notice framework in Section 8 and Section 12(2)(e) considers a consent to be valid only if it is capable of being withdrawn, this right must be recognised as a separate right in Chapter VI so that a data principal has remedies available as per the procedure laid down by Section 28.
CONNECT | PROTECT | RESPECT

www.cyberpeace.org | secretariat@cyberpeace.net

facebook.com/cyberpeacefoundation twitter.com/cyberpeacengo youtube.com/cyberpeacefoundation