(Draft) Personal Data Protection Bill 2018: Rights and entitlements

Beni Chugh
Research Associate, Dvara Research

CUTS, Capacity Building Workshop on Raising Consumer’s Awareness Level On Data Protection And Privacy And Impact Of Personal Data Protection Bill On Them Jaipur, 18-19 July, 2019
Our conversation today

1. Data protection: First-principles
2. Evolution of data protection regime in India
3. The (draft) Personal Data Protection Bill (PDP Bill), 2018
4. Users’ rights under the (draft) PDP Bill
5. Obligations under the (draft) PDP Bill
6. Grievance Redress under the (draft) PDP Bill
7. The proposed data protection authority
8. Some concerns
Data protection: First-principles
1. Data protection: First-principles

What is personal data?

Se. 2(29) of the (draft) Bill 2018, defines personal data as:

(29) "**Personal data**" means data about or relating to a **natural person** who is **directly or indirectly identifiable**, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, or any combination of such features, or any combination of such features with any other information;
1. Data protection: First-principles

Why protect personal data?

- To uphold the fundamental *right to privacy*
- To protect against the *harms from the misuse of personal data*
- To protect *competition in markets*
Right to Privacy: People care deeply about their personal data

Privacy on the Line, 2018
The need to protect personal data: Harms

Harms from misuse of personal data:

- Direct financial loss
- Discrimination
- Exclusion
- Limiting Consumer Choice
- Fraud
1. Data protection: First-principles

**How to protect personal data?**

Data protection legislations are being adopted by nations across the world.

As in June 2018:

- The European Union’s General Data Protection Regulation (GDPR) was implemented in May 2018.
- 126 nations had an active data protection regulation
- 34 nations were deliberating on a draft data protection bill

Ironically, India belongs to both groups.
1. Data protection: First-principles

How to protect personal data?

126 Countries with data privacy Laws (to June 2018)
2. Evolution of data protection regime
2. Data protection regime in India: Evolution

- 2000: Information Technology Act
- 2011: Reasonable security practices and procedures and sensitive personal data or information
- Jul 2017: Constitution of a Committee of Experts to deliberate on a data protection regime in India
- Aug 2017: Right to privacy, further impetus to data protection
- Nov 2017: {White Paper of the Committee of Experts on a Data Protection Framework for India}
- Aug 2018: (Draft) Personal Data Protection Bill, 2018
3. (Draft) Personal Data Protection Bill, 2018
The draft PDP Bill recognises *four* key stakeholders:

- **Data Principal**: You and I
- **Data Fiduciary**: Bank, Google, Facebook
- **Data Processor**: Mu Sigma, Fractal Analytics
- **Data Protection Authority**: Law-making powers

**Rights**: Chapter VI  
**Obligations**: Chapter II  
**Transparency & Accountability Measures**: Chapter VII  
**Law-making powers**: Chapter X, XI, XIII
4. Rights of data principals
The (draft) PDP Bill vests *four rights* in the data principal:

- Right to confirmation and access
- Right to correction
- Right to data portability
- Right to be forgotten
4.1 The right to confirmation & access

It empowers the data principal to seek from the data fiduciary:

- a confirmation if their data is being or has been processed
- a brief summary of the personal data
- a brief summary of the activities undertaken by the fiduciary

The fiduciary must provide this information in a clear, concise, easy-to-understand manner.

This right is important because

- You cannot protect until you know what is happening to your data
- You cannot withdraw consent, seek redress etc.
- It lays the foundation for exercising other rights and examining obligations
4.2 The right to correction

Under this right:

- Data principal can dispute the quality of their personal data
- They can get it (i) corrected, (ii) completed and (iii) updated
- Data fiduciary must reject correction requests in writing
- Data principal can appeal against rejection
- Data fiduciary must get it corrected across entities

This right is important because:

- Quality of data impacts the decision made using the data
- It can affect if you get your ration, a loan etc
- The case of Sani Tutti
- The case of Judy Thomas and Judith Upton.
The case of Sanni Tuti

Different names on all her documents. Is this being counted as ‘identity fraud’? #AadhaarFail (4/22)

Sanni Tuti has different names on her ration card, voter ID and Aadhaar card.

Her ration card was cancelled because of this mismatch.

Is this being counted as ‘identity fraud’?

Salgadih, Khunti

Credits: Priya Dua
4.3 The right to data portability

Under this right, the data principal:

- must receive the data they shared with a data fiduciary in a structured, machine-readable format
- can instruct a data fiduciary to transfer data to another fiduciary
- subject to three exceptions

- Data offers competitive advantages
- Having access to big data can encourage monopolistic practices and abuse of dominant position
- This decreases consumer surplus and potentially consumer welfare
4.4 The right to be forgotten

The data principal can restrict or stop sharing their personal data with a data fiduciary, if:

- the data has served its purpose
- consent for sharing data is being withdrawn
- is in contravention of the law

An Adjudicating Officer determines if the right can be exercised

- It upholds data principal’s autonomy and control of their personal data
- It obliges organisations to fulfil their obligations
5. Obligations: Data fiduciaries and data processors
5.1 (Draft) PDP Bill: Obligations of data fiduciaries, data processors

The draft Bill places 8 obligations on the data fiduciaries and data processors:

1. Fair & Reasonable Processing
2. Purpose Limitation
3. Collection Limitation
4. Lawful Processing
5. Notice
6. Data Quality
7. Storage Limitation
8. Accountability
5.2 (Draft) PDP Bill: Transparency and accountability mechanisms

Additionally, the draft Bill places 11 accountability and transparency processes:

1. Privacy by design
2. Transparency
3. Security Safeguards
4. Personal Data Breach
5. Data Protection Impact Assessment
6. Record-Keeping
7. Data- Audits
8. Data Protection Officer
9. Processing by entities other than data fiduciaries
10. Classification of data fiduciaries into significant data fiduciaries
11. Grievance redress
6. Grievance Redress
6.1 “Harm” under the PDP Bill 2018

“Harm” includes—

i. bodily or mental injury;
ii. loss, distortion or theft of identity;
iii. financial loss or loss of property,
iv. loss of reputation, or humiliation;
v. loss of employment;
vi. any discriminatory treatment;
vii. any subjection to blackmail or extortion;
viii. any denial or withdrawal of a service, benefit or good resulting from an evaluative decision about the data principal;
ix. any restriction placed or suffered directly or indirectly on speech, movement or any other action arising out of a fear of being observed or surveilled; or
x. any observation or surveillance that is not reasonably expected by the data principal.
6.2 Grievance redress: Trigger and process

- Every data fiduciary must have a grievance redress mechanism in place
- Grievance can be raised if there is a violation that may cause harm to the user
- Data fiduciary must resolve complaints within 30 days
- The data principal can escalate the matter to the Data Protection Authority
7. Data Protection Authority
The proposed Data Protection Authority

- Monitoring & Enforcement
- Legal Affairs, Policy & Standard Setting
- Research & Awareness
- Inquiries & Grievance

Data Protection Authority

Adjudication Wing

Appellate Tribunal

- Appeals against orders of the appellate tribunal will be to the Supreme Court of India.
Some concerns

1. The aspiration for a “data fiduciary” paradigm falls short in application
2. Data principals are afforded a limited set of rights
3. The draft PDP Bill creates high barriers to exercise the rights by data principals
4. The grievance redress framework is burdensome and limited for users
5. The definition and usage of “harm” in the draft Bill limits user protections and rights
6. The draft Bill disincentivises and penalises withdrawal of consent
Thank you.

Beni Chugh
Research Associate, Dvara Research