How India Plans to Protect Consumer Data

Table Of Contents

Personal Data Protection Bill (DPB)

- Important development for global managers. The digital economy in India is expected to reach a valuation of $1 trillion dollars by 2022 - and it will attract numerous global players who must comply with DPB.
- Indian DPB carries additional provisions beyond the EU regulations. Because India is a nation state, it would treat the data generated by its citizens as a national asset, store and guard it within national boundaries, and reserve the right to use that data to safeguard its defense and strategic interests
- The issues raised here server as a primer for what businesses need to keep in mind about India's new regulation, and increase in **data protection regulation** around the world

Privacy As A Fundamental Right

- Privacy is a constitutional right of Indian citizens
- Intentions to protect, safeguard citizen's privacy rights by controlling the collection, security, storage, sale, and exploitation of these data
- Many of those digital firms would have to rethink their business models if they can no longer collect, exploit, retain, and sell user data as profitably as before

User Content

- DPB requires that a digital company must obtain explicit permission from a user before collecting their personal data
- Compliance is tricky

- For example,
  - Uber
  - Amazon
- Data tracking
- Security
- Obtain user permissions
- "Data fiduciaries"

Ownership Of Personal Data

- In principle, DPB proposes that the data provider is the owner of their own personal data
- In the physical world, a property owner can ask for return of their property
- For example,
  - When a person requests deletion of all of their information after they cease to be a Facebook member

Three Classes Of Data

Three categories include,

- **Sensitive**: Includes financial, health, sexual, genetics, transgender, caste, religious belief
- **Critical**: Includes information that the government stipulates from time to time as extraordinarily important, such as military or national security data
- **General**: Not defined, but contains the "remaining" data

`Splinternet`.

Data Sovereignty

- DPB would treat citizens' data as a `national asset`
- DPB differs from GDPR, which imposes no locational storage requirements
- One implication of the new policy is that when the government demands its citizens' data, in case of foreign attacks and surveillance

National Interests

While placing a large emphasis on citizens' privacy, DPB disregards privacy rights in certain cases. It states, "All or any of the provisions of this Act shall not apply to any agency of the Government in respect of processing of such personal data…".

That is, various public sector entities of the government of India will not require individuals' consent to obtain their personal data when responding to the secu-

rity of the state, detection of any unlawful activity or fraud, and epidemic and medical emergencies.

Critics argue that these data can be potentially misused by the government for unintended uses such as political surveillance.

Recall Apple's refusal to unlock an iPhone.

Verification Tag

DPB requires that all digital companies must identify their users and tag them into three categories to reduce trolling.

- Users who have verified their registration and display real names
- Users who have verified their registration, but have kept their names anonymous
- Users that have not verified registration

This would be a first regulation of its kind in global social media.

Note that Facebook has more than 100 million fake accounts and faces of dilemma of continuing as is, attempt to verify them, or delete those accounts.

Compliance & Enforcement

DPB proposes steep penalties for noncompliance.

Penalties could reach $700,000 or 2% of a company's global revenues, whichever is higher.

Penalties for data shared without consent, which double.

These penalties, which are based on multinationals' global income, and potential jail sentences for officers of digital companies, imply that DPB regulations cannot be taken lightly.

Taxing Digital Companies

Multinational digital companies can easily transfer their income to tax havens and avoid paying taxes to local governments, with no fear of confiscation of their properties.

This would lower the likelihood that digital companies can get away with paying little or no taxes to the local governments.

Other Issues

The DPB applies to all businesses that collect personal data, not just digital businesses. For example, **John Deere** collects and processes **data** obtained from its farm equipment. Whether DPB applies to,

- Tractors with sensors

- Whether data belongs to farmers
- Benefits of farm data

Uniform standards, similar to ISO 9000, would promote global commerce.

References

- How India Plans To Protect Consumer Data