Legislating for Data Protection

What is the issue?

\n\n

\n
- Supreme Court recently ruled privacy as a fundamental right.
\n
- This has triggered calls for data localisation in India.
\n

\n\n

Why data localisation?

\n\n

\n
- Currently there is no law guaranteeing either privacy in general or data security in particular.
\n
- Most companies collecting data in India are MNCs that operate through local subsidiaries.
\n
- The data collected is generally stored on servers located abroad.
\n
- Such data is mined and analysed extensively and, quite possibly, shared with affiliates without any legal hurdle.
\n
- The government is hence contemplating a law to mandate data-localisation.
\n
- This would require data of Indian users to be stored on servers within India and hence be subject to Indian jurisdiction.
\n

\n\n

What are the concerns?

\n\n

\n
- Relatively few countries have legislated for data localisation and such laws

are perceived to be undemocratic in character.
\n
- Indian servers are also not secure - given the occurrence of multiple leaks on a massive scale.
\n
- Locally-storing data provides the government with full access to demand and receive data at will.
\n
- Given the opacity of Indian surveillance protocol, data localisation could easily lead to serious privacy violations.
\n

\n\n

How can the future be best approached?

\n\n

\n
- The Supreme Court ruling makes it imperative that a strong privacy law with robust safeguards is swiftly passed by Parliament.
\n
- European Union has opined that data belong to the individual citizen who has generated it – and has legislated accordingly.
\n
- Implementing this in the Indian context will require a carefully drafted privacy code that is passed into law.
\n
- The government should work to ensure that data generated by Indians should be controlled by Indian laws, regardless of location.
\n

\n\n

\n\n

Source: Business Standard

\n