Data localisation is no solution-The data protection bill is an opportunity for India to be a partner under the CLOUD Act

Posted at: 03/08/2018

Highlights

Calls for data localisation are not new.

- The Justice Srikrishna Committee in its report accompanying the draft **Personal Data Protection Bill** released on July 27 notes that eight of the top 10 most accessed websites in India are owned by U.S. entities.
- This reality has often hindered Indian law enforcement agencies when investigating routine crimes or crimes with a cyber element. Police officials are forced to rely on a long and arduous bilateral process with the U.S. government to obtain electronic evidence from U.S. communication providers.

User data

- The Bill calls for a copy of user data to be mandatorily localised in India, believing that it will "boost" law enforcement efforts to access data necessary for investigation and prosecution of crimes.
- However, the law will be counterproductive, hurting law enforcement efforts and undermining user rights in the process.
- The last few months have witnessed an amplification in data localisation demands, with the Reserve Bank of India, to take one example, calling for local storage of financial data.

A fundamental error by SriKrishna Committee is to believe that location od data should determine who has access to it.

- Indian Law enforcement relies on outdated Mutual Legal Assistance Treaty(MLAT) as U.S law effectively bars companies from sharing data without a prior warrant and this scenario will not change even after technology companies relocate Indian data to India.
- However localisation of India data is useful in boundaries of the country only w.r.t.crimes ,prevalent concerns around transnational terrorism, cyber crimes and money laundering pushing to continue relying on cooperative models like the MLAT process because of lack or insufficiency of data.

The Clarifying Lawful Overseas Use of Data (CLOUD) Act, passed by the U.S. Congress earlier this year, seeks to de-monopolise control over data from U.S. authorities.

- The law will for the first time allow tech companies to share data directly with certain foreign governments.
- This, however, requires an executive agreement between the U.S. and the foreign country certifying that the state has robust privacy protections, and respect for due process and the rule of law.

The draft Bill was an opportunity to update India's data protection regime to qualify for the CLOUD Act.

- The Bill, while recognising principles of legality, "necessity and proportionality" for data processing in the interest of national security and investigation of crimes, fails to etch out the procedural rules necessary for actualising these principles.
- Even rudimentary requirements such as a time limit for which data can be stored by law enforcement are missing from the Bill.

With the highest number of users of American technology offerings and a high number of user data requests, second only to the U.S., India is a clear contender for a partnership under the CLOUD Act.

Source: The Hindu