Data localisation is not enough

Calls for data localisation are not new. It has been a mainstay of Indian policymakers' demands from foreign technology companies. 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. The committee seeks to correct this.

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. If passed in his form, 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 that the Srikrishna Committee seems to have made is in its belief that the location of data should determine who has access to it. The reason that Indian law enforcement relies on an outdated Mutual Legal Assistance Treaty (MLAT) process to obtain data stored by U.S. companies is because the U.S. law effectively bars these companies from disclosing user data to foreign law enforcement authorities. Technology companies are allowed to share data such as content of an email or message only upon receiving a federal warrant from U.S. authorities. This scenario will not change even after technology companies relocate Indian data to India.

The committee too acknowledges that data localisation is not a perfect solution. Its decision is borne of hope that when questions of data access are determined, their storage here will give rise to a strong Indian claim. This is not an unreasonable expectation, albeit a weak one.

Even if Indian authorities force compliance from U.S. companies, it will only solve a part of the problem. The draft bill mandates local storage of data relating to Indian citizens only. Localisation can provide data only for crimes that have been committed in India, where both the perpetrator and victim are situated in India. Prevalent concerns around transnational terrorism, cyber crimes and money laundering that the committee rightly highlights will often involve individuals and accounts that are not Indian, and therefore will not be stored in India. For investigations into such crimes, Indian law enforcement will have to continue relying on cooperative models like the MLAT process.

Questions around whether access to data is determined by the location of the user, location of data or the place of incorporation of the service provider have become central considerations for governments seeking to solve the cross-border data sharing conundrum. 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.

On procedural questions of law enforcement access, the draft Bill falls very short. Even if it were to be passed, legacy provisions such as Section 91 of the Code of Criminal Procedure (empowering

police to access any “document or thing”) will continue to apply — bereft of review or oversight by a judicial or independent authority. The Committee, while imposing data localisation, should have also necessarily tackled how this data will be obtained by police authorities — whether within its mandate or not.

The CLOUD Act creates a potential mechanism through with countries such as India can request data not just for crimes committed within their borders but also for transnational crimes involving their state interests. Access to data would be determined by where the user is located and the reasonableness of claim that a country has in seeking her data. 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.

In other words, the Committee has sought to localise data for law enforcement but categorically refused to afford this data any procedural protection. The Committee has instead placed the onus on Parliament to enact another comprehensive legislation for surveillance reform.

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. If New Delhi recognises this opportunity and reforms laws around government access to data, both the Indian user and law enforcement will be better served in the long run.

Madhulika Srikumar and Bedavyasa Mohanty are lawyers and Associate Fellows with Observer Research Foundation, New Delhi

END