NUS National University of Singapore | ISAS Institute of South Asian Studies

ISAS Brief
No. 929 – 9 May 2022

India's New VPN Rules

Karthik Nachiappan

Summary

The Indian government's new policy will force virtual private networks (VPNs) to retain user data for five years. This mandate will likely make it difficult for VPN companies to manage and for users to utilise the service in India.

The Indian government has been lumbering slowly to pass and enact a data protection bill since 2017. Several efforts have been taken without a final bill that could be put to vote, including committees to study and draft a bill grounded on privacy, several bills to protect data and another joint parliamentary committee to suggest how the bill should be improved. Despite these moves, we still do not have a final data protection bill or clarity on where things are now. However, this delay has not stopped the government from issuing directives to manage and control domestic data.

On 4 May 2022, the Indian government mandated virtual private network (VPN) companies operating in India to collect users' data for government use or else face punitive action, including ceasing operations. The move suggests that the government will unlikely move far from creating a data protection framework that facilitates the control of personal data generated in India, irrespective of constitutional and political considerations. The VPN directive does not come as a surprise for those closely watching India's data protection trajectory. Moreover, it reveals that the delay toward a final data protection bill could be driven by cyber security considerations, given the rising spate of cyber incidents and attacks. Since 2018, India has experienced a surge in cyber breaches, attacks and crime. Last year, five serious data breaches led to the data of more than 110 million users leaked online, with the costs of such breaches and incidents mounting. Indeed, the VPN order was announced by India's Computer Emergency Response Team (CERT-IN), an agency under the Ministry of Electronics and Information Technology that deals with security threats to India's internet. The ministry's directive is slated to take effect from 27 June 2022, though government officials may delay implementation to allow time for compliance.

Until now, it was speculated that the delay in passing the data protection bill was largely due to parliamentary procedure to ensure that all actors were given due consideration before the framework was finalised. However, there is an indication that the government softened its initial position on data localisation in the bill due to foreign, notably big tech, pressure to make it easier for them to process and ship data they collect from Indian users. Left uncovered was the cybersecurity story, which now receives scrutiny through these rules. India's weak cybersecurity could potentially affect the efficacy and scope of the data protection bill since it involves the safety and integrity of data.

Specifically, the CERT-IN order requires VPN companies to collect extensive customer data and hold it for five years. The data collected will include contact details, validated physical and IP addresses, VPN usage patterns and personally identifiable information. Failure to

furnish required information could result in punitive action for these companies, including closure. These rules will also apply to all cloud service providers and virtual private service providers. In addition to this new order, the government has asked VPNs, service providers, intermediaries and data centres to report any breaches or leaks within six hours of them being flagged, undoubtedly a difficult task. Most VPNs, in fact, operate without collecting such personal details and provide services that circumvent the collection of personal data. India's new rules could potentially make it very difficult for them to operate.

VPN operators like Nord, Proton, Express and Surfshark have rejected the rules and government's reasoning. All these providers have made it clear that they will not comply with these new rules because it is technically infeasible for them to do so. Some of these companies could also pull out of India to avoid compliance or because they do not have any physical presence in India to comply and follow up with the government. Windscribe, one VPN operator, criticised the rules for being more stringent than that of China and Russia. It is worth watching whether these VPN services create India-specific VPNs that will adhere to the government's new directive since Indian corporate businesses, especially from the information technology sector, are major clients of these VPNs and cloud-based service operators and if they will require their services despite new rules. Indian firms will need these services to continue managing and conducting their operations, which makes living without a VPN unviable.

However, from a data protection perspective, these VPN moves, which may appear stringent or coercive to some, mesh with the Indian government's desire to place the state at the centre of all data collection nodes before creating a framework that embeds those activities. Privacy appears non-existent as a priority or objective. Instead, the government is focused on digital and cyber security. It appears that hackers and cyber mercenaries are using VPNs to launch cyber-attacks on government agencies and private firms. These new directives, however broad and onerous, are meant to deter and mitigate those attacks by forcing VPNs and related providers to keep a record of their user activities online.

. . . . .

Dr Karthik Nachiappan is Research Fellow at the Institute of South Asian Studies (ISAS), an autonomous research institute at the National University of Singapore (NUS). He can be contacted at isaskn@nus.edu.sg.
The author bears full responsibility for the facts cited and opinions expressed in this paper.