Does the Personal Data Protection Bill, 2019, protect citizens' privacy from government surveillance?

As the Joint Parliamentary Committee considers the Personal Data Protection Bill, 2019, MediaNama will publish a series of articles from legal experts focussing on the key aspects of the Bill and how they will affect users and companies. This is the eighth article in the series. Read our extensive coverage of the Bill here.

By Pallavi Bedi

*

A government agency buys surveillance software from a foreign company. It then plants the software in the devices of Indian citizens. The device company, that also operates a number of apps, discovers the software and sues the foreign company. Can the DPA investigate the government agency?

The suit filed by WhatsApp in a Northern California court against the Israeli cyber-intelligence company, NSO Group Technologies, laid bare the nefarious intrusions of the global surveillance industry into the protection of civil liberties and the trajectory of geo-politics narratives. WhatsApp alleged that the NSO group had deployed the Pegasus spyware to conduct targeted surveillance on the cellphones of over 1,400 lawyers and human rights activists all over the world, including from India.

Given NSO's statements claiming that they only sell services to state governments, there was widespread suggestion that the Indian government had deployed Pegasus to target dissenters against the ruling government. On November 29, 2019, the IT Minister, Ravi Shankar Prasad failed to categorically deny that the Indian government had used Pegasus to spy on its own citizens, instead merely claiming that "standard operating procedures have been followed."

The government derives its power and authorisation to conduct surveillance from Section 69 of the Information Technology Act (IT Act), read with the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information Rules), 2009 (IT Rules). The rules lay down the procedure to be followed by the government agencies to undertake electronic surveillance. It is pertinent to note that the IT Act — under Section 43 and Section 66 — penalises any unauthorised access to computer systems, and the government has not been granted any exception.

On November 19, 2019 in response to a specific question on whether the government was tapping WhatsApp's calls and messages, the Minister of State in the Ministry of Home Affairs, G. Kishan Reddy, referred to the procedure prescribed under Section 69 of the IT Act and under Rule 5 of the Indian Telegraph Act and stated that only 10 agencies authorised by the Ministry of Home Affairs

were permitted to undertake any interception or monitoring.

The global surveillance industry is a dangerous, strategic conglomeration of states adopting an increasingly authoritarian approach to the use of technology, and the private sector are willing allies in a bid to rake up profits at the expense of civil liberties. The possibility of entrenched networked surveillance today makes this scenario a critical one for understanding the efficacy of the proposed Personal Data Protection Bill. Can its provisions and the authorities empowered by it genuinely preserve privacy in India today?

How will the Central Government, WhatsApp and NSO be classified under the Bill?

The Central Government and WhatsApp can be classified as data fiduciaries under the Bill as they determine the means and purposes of processing of personal data. The users of WhatsApp in India will be regarded as 'data principal'.

The jurisdiction of the Bill is country-agnostic as long as the data fiduciary 'offers services to data principles within the territory of India' and therefore, WhatsApp will come within the ambit of the Bill and it will be required to comply with the obligations specified in the Bill.

On the other hand, the NSO may not be regarded as a data fiduciary as its role appears to be limited to providing the surveillance tools to the State — it does not determine the purpose and means for which such surveillance tools will be used — that is left to the State.

Can the DPA investigate a government agency and WhatsApp?

The Bill establishes a Data Protection Authority (DPA) to 'protect the interests of the data principal, prevent any misuse of personal data and ensure compliance with the provisions of the Bill'. Under the Bill, the DPA has the authority over the processing of personal data by private data fiduciaries as well as the State.

An important obligation of the data fiduciary under the Bill is to maintain transparency while processing personal data and as part of this obligation, Section 23 (1)(e) requires the data fiduciary to inform the data principal about the right to file a complaint against it before the DPA. Further, section 53 (1) provides that the DPA can either *suo-motu* or on a complaint received by it inquire into the activities of any data fiduciary, if the activities are being conducted in a manner which are detrimental to the interests of the data principal.

Once the complaint is received, the DPA is required to issue a written order appointing an Inquiry officer responsible for conducting an inquiry and submitting a report to it. Upon receipt of the report, the Bill specifies the measures that the DPA can undertake — these range from reprimanding the data fiduciary to temporarily suspending the activities of the data fiduciary which are in

contravention of the Bill.

How will this work in practice?

In theory, the Bill provides the framework for any data principal to file a complaint before the DPA against the actions of a government agency and WhatsApp and for the DPA to initiate an inquiry. However, the extensive exemptions powers given to the Central Government under the Bill belies this expectation.

The 2018 Bill sanctioned processing of personal data by intelligence agencies and law enforcement officials and exempted such authorities from certain provisions of the Bill. However, such sanction to either intelligence officials or law enforcement agencies was subject to it being (a) authorised by law; (b) in accordance with the procedure laid down by the law; and (c) necessary and proportionate. This four-step process embeds the principle laid down by the Supreme Court in Right to Privacy judgement (*Puttaswamy v. Union of India* [2017]). This was regarded as a first step towards determining the surveillance powers of the State and the expectation was that the government would further strengthen the provision to streamline and regulate the surveillance apparatus.

However, the present Bill has the opposite effect — instead of regulating surveillance, it has augmented the government's surveillance power. Section 35 now provides that the Central Government can exempt any agency from **all or any provision** of the Bill if it is necessary or expedient to do so in the interests of (a) sovereignty and integrity of India, national security, friendly relations with foreign states, and public order or (b) for preventing incitement to the commission of a cognizable offence relating to (a). The four-stage test proposed in the Puttaswamy judgement has been done away with. Further, the procedure to be employed and the oversight mechanism to be followed by the exempted government agency (exempted by the Central Government under this provision) will be prescribed in the future

By virtue of Section 35, the government can exempt the surveillance and law enforcement agencies from the jurisdiction of the DPA. In addition, the government can also exempt such agencies from all the transparency and accountability requirements specified in the Bill. Therefore, the affected data principal may never be notified about the processing of her personal data by law enforcement agencies and/or surveillance agencies, and therefore will not be able to file a complaint before the DPA.

An essential obligation of the data fiduciary under the Bill is to implement necessary security safeguard features considering the nature and purpose of processing of personal data. WhatsApp could argue that it has employed end-to-end encryption for all messages and calls by default and that it has sought a permanent injunction banning NSO from using its service, thereby complying with this requirement.

Therefore, despite having jurisdiction, in practice, the DPA will be unable to

adequately protect the rights of the data principal. This means that alternate means of preventing the development, testing, sale and transfer of surveillance technology will need to be devised at the national and global levels.

*

Pallavi Bedi is a senior policy officer at the Centre for Internet & Society. This article was written with inputs from Arindrajit Basu.

Edited by Trisha Jalan