

PEGASUS: SC PANEL TELLS PEOPLE TO REPORT IF THEY WERE TARGETS

Relevant for: Security Related Matters | Topic: Basics of Cyber Security and related matters

No snooping: Congress supporters protesting against the use of Pegasus spyware to snoop on activists. File Photo

The technical committee examining the Pegasus spyware allegations has issued a public notice inviting citizens to come forward if they suspect that their mobile phones or instruments have been infected with the Israeli military grade malware.

The committee, overseen by former Supreme Court judge, Justice R.V. Raveendran, said citizens should make it clear whether they would let the committee further examine their phones or instruments if “reasonable cause” is found that they are infected.

Citizens who believe they were victims of Pegasus snooping should write to the technical committee at inquiry@pegasus-india-investigation.in by January 7 noon. They should give detailed reasons to substantiate their suspicions. News reports had said a cross-section of people from journalists, activists, parliamentarians, government officials, lawyers and even court staffers were targetted using Pegasus.

In case the suspicions ring true and deserve further examination, the mobile phones and instruments would be collected by the committee in Delhi and digital phone images of the records collected would be provided to their owners.

Wide mandate

The job cut out for the committee is to “enquire, investigate and determine” whether the “Pegasus suite of spyware was used on phones or other devices of the citizens of India to access stored data, eavesdrop on conversations, intercept information and/or for any other purposes”. The committee also has to get the “details of the victims and/or persons affected by such a spyware attack”.

The other questions for the committee include whether Pegasus was used by the Centre or State or any of their agencies against their own citizens, and if used, was it authorised and under what law or procedure.

The Supreme Court Bench led by Chief Justice of India N.V. Ramana wanted the committee to dive deep into the first public signs of the alleged use of the military-grade spyware years ago. The court had wanted the committee to dig up the steps taken by the government “after reports were published in the year 2019 about hacking of WhatsApp accounts using the Pegasus suite of spyware”.

The court also wants the committee to use its expertise to test the existing surveillance laws and procedures to see how much they value and protect citizens’ privacy. The court said the committee should come up with recommendations to prevent State and non-State players from invading the fundamental right of privacy of citizens through illegal surveillance mounted on them.

The court has also asked the Justice Raveendran panel to come up with suggestions for

enhancing and improving the cyber security of the nation and its assets. Noting that there should not be any delay in protecting citizens from malicious spyware attacks, the court had even asked the committee to suggest an *ad hoc* arrangement that could be passed by the Supreme Court as an interim measure until the Parliament came up with a law.

[Our code of editorial values](#)

END

Downloaded from **crackIAS.com**

© **Zuccess App** by crackIAS.com