GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 1951
TO BE ANSWERED ON: 05.12.2019

NSO SPYWARE SCANDAL

1951. DR. ABHISHEK MANU SINGHVI:

Will the Minister of Electronics & Information Technology be pleased to state:-

(a) the details of all the steps taken after the NSO Pegasus spyware scandal;

(b) whether the Ministry is aware of all the companies that sell such software or provide services; and

(c) what steps the Ministry has taken to ensure the bulwarking of such spywares in the country?

ANSWER

MINISTER FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI RAVI SHANKAR PRASAD)

(a): On 31st Oct., 2019, there was news in Indian media reporting breach of data of few Indians via WhatsApp through a spyware named Pegasus developed and marketed by an Israel based company namely NSO. Ministry of Electronics & Information Technology (MeitY) took cognizance of the news reports and sought a report from the WhatsApp through an email sent to them on 1st November and seeking WhatsApp response by 4th November. WhatsApp responded on 2nd November 2019 communicating the aspects relating to exploitation of a vulnerability in their platform by a spyware called Pegasus, developed by Israeli agency named NSO. Once the official response was received from WhatsApp, the Indian Computer Emergency Response Team (CERT-In) issued a notice on 9th Nov 2019 and sought clarifications from WhatApp. WhatsApp had responded to the initial notice on 18th Nov 2019. CERT-In has also issued a notice to NSO group. The response from WhatsApp was received on November 18, 2019 and further clarifications and technical details were sought on 26th November, 2019. CERT-In has also sent a notice to NSO Group on 26th November, 2019 seeking details about the malware and its impact on Indian users.

(b): No, Sir.

(c): The Indian Computer Emergency Response Team (CERT-In) is tracking cyber threats affecting users and issuing advisories to users regarding best practices to be followed for protection of information while using Social Media and securing mobile devices.

.

****