Dr Shashi Tharoor,
Hon'ble Chairperson, and

Members,
Parliamentary Standing Committee on Information Technology

comit@sansad.nic.in, office@tharoor.in, legislation@tharoor.in

November 19, 2019

Dear Sir and Respected Members of the Parliamentary Standing Committee,

Re: Letter to the Parliamentary Standing Committee on Information Technology from Civil Society Activists and Human Rights Defenders Targeted by NSO-Pegasus Spyware seeking detailed probe into the cyber-attacks on Indian citizens

We, the undersigned, are a group of human rights defenders – academics, cultural activists, journalists, lawyers, researchers and students - united by our commitment to democratic rights, constitutional freedoms and the rule of law. Individually and collectively, we have actively engaged with issues of public concern. Our commitment to democracy, justice and the values enshrined in the Constitution of India has meant standing in solidarity with those facing attacks on their life, liberty and livelihoods. This involves defending the rights of farmers, workers and marginalised communities like Adivasis, Dalits, and Muslims as well as the rights of those who have been wrongfully targeted and arrested in the so called 'Bhima-Koregaon case'.

Today, we wish to bring to your notice one other circumstance that unites us. Over the last month, we have all received official communication from WhatsApp and Citizen Lab informing us that our mobile devices have been targets of highly sophisticated cyber-attacks. According to this official communication, spyware has been implanted in our mobile devices through WhatsApp's video calling service. This compromises our digital security and makes it possible for the attacker to gain access to and tamper with the functioning of our mobile devices and as a result, all other electronic devices to which they are linked.

WhatsApp has traced this attack to a spyware called Pegasus which is the flagship product of the Israel based NSO Group and its parent company Q Cyber Technologies, both of which are alleged to have close ties to Israel's security agencies. Pegasus is possibly one of the most sophisticated spyware available today. Once installed on a mobile device, Pegasus allows a remote operator to have access to all of the device's contents, including call logs, contact lists, internal memory, media files, passwords, text messages and voice calls. Furthermore, the spyware allows the remote operator to

switch-on the phone's camera and microphone at will and capture the real-time activity in the immediate vicinity of the mobile device. These are only some of the capabilities of this software of which we are aware.

Reports in national and international media based on investigations by digital security experts and independent researchers have revealed extremely disturbing details of the operations of the NSO group and its links to the Israel's "deep state". The NSO Group has itself claimed that Pegasus software is sold only to security agencies of sovereign governments. Deploying Pegasus for large-scale surveillance is quoted to cost several millions of dollars, and requires manipulation of the national telecommunications infrastructure. These and many more technical details are now on the record in the case filed by WhatsApp against the NSO Group in a USA court.

As aware and active members of civil society, we believe that our rights, including our right to privacy, free speech and online assembly are respected, assured and protected by the Government of India. These revelations of surveillance using software procured from foreign private companies and that our intimate details, personal conversations, financial transactions and private lives were and are being tracked and monitored is deeply disturbing. This snooping is a violation of our fundamental right to privacy and compromises our safety and security, as well as the privacy, safety and security of our families, friends, colleagues, clients and any and every citizen who has communicated with us through our mobile devices.

We are sure that you will agree that this kind of surveillance is a flagrant violation of our rights as citizens and violates the letter and spirit of our democratic traditions, civil liberties and constitutional rights and freedoms. The implications of such surveillance are greater than the violations of the rights of targeted individuals. It also has a chilling effect on the freedom of speech and activities of civil society as a whole.

A statement from Shri Ravi Shankar Prasad, Minister for Information Technology on 31 October 2019 adds to our concerns. It suggests that this targeting of human rights defenders and civil society activists has been carried out without the knowledge and permission of the Government of India. If this is true, the Pegasus attacks have serious implications for national security. The fact that foreign private companies and other foreign actors have penetrated the national telecommunications infrastructure without detection by Indian security agencies, and now possess the ability to access and extract the most intimate details of so many Indian citizens, is a violation of international norms and is a direct attack on our national sovereignty.

It is, therefore, incumbent on the government to act immediately and decisively against these flagrant violations of fundamental rights and freedoms of Indians by dubious actors and entities with possible links to foreign governments.

In view of the above, we request the committee to take two actions. First, at present, some of us are willing and forthcoming to provide oral testimony to the Standing Committee. We request you to kindly consider this. Second, we urge the Members of the Standing Committee to summon relevant government departments to place the

following questions with a view towards gaining greater factual accuracy around this grave injury to our personal privacy and digital security.

1. Which agencies and entities are carrying out this targeted and unauthorised surveillance of Indian citizens?
2. Are sections of the Indian government, central or state, involved in deployment of the Pegasus software?
3. Has public money been expended for these illegal and unauthorised attacks? Who authorised this expenditure?
4. Are central security agencies aware of the presence of NSO Group employees and operatives in India? Have these operatives entered the country legally?
5. Who were the individuals under surveillance by the Central or State agencies using this or other related technology?
6. What steps is the government taking to identify and bring to book the entities involved in the Pegasus attacks and other possible instances of illegal and unauthorised surveillance of Indian citizens?
7. What steps is the government taking to identify and repair the breaches in the national telecommunications infrastructure and protect it against any further attacks?
8. In the interests of transparent, accountable and responsive governance, we urge you to also make public the details of the companies, agencies and other entities authorised by the Government of India to carry out surveillance in accordance with legal provisions. What are the terms and conditions that govern the operations of these agencies? What are the arrangements for monitoring and overseeing their work?

We look forward to your responses to the above questions. Placing these details in the public domain would contribute towards reassuring the public that the Government of India is committed to protecting the rights and freedoms of Indian Citizens from being violated by illegal and unauthorised actors. We believe that this Standing Committee will conduct a thorough probe, report on the same and ensure appropriate action is taken.

We, the undersigned, remain available to assist the Standing Committee in its endeavour to safeguard the privacy and security of all citizens, including academics, activists, human rights defenders, journalists and lawyers, who are facing growing threats to their life and liberty.

For the purposes of correspondence phone numbers, postal addresses, email addresses given below be used.

Dated 19 November, 2019 and electronically approved/signed by:

<PERSONAL DETAILS REDACTED>

1. Ajmal Khan
2. Alok Shukla
3. Anand Teltumbde
4. Ankit Grewal
5. Asish Gupta
6. Balla Ravindranath
7. Bela Bhatia
8. Degree Prasad Chouhan
9. Jagdish Meshram
10. Mandeep Singh
11. Nihalsing B Rathod
12. Rupali Jadhav
13. Shalini Gera
14. Sushil
15. Vidhya
16. Vira Sathidar
17. Vivek Sundara