FOUNDER PRESIDENT
VIDUTHALAI CHIRUTHAIGAL KATCHI (VCK)

सत्यमेव जयते

MEMBER OF PARLIAMENT
CHIDAMBARAM CONSTITUENCY - TAMIL NADU
MEMBER : • STANDING COMMITTEE - COAL AND STEEL
• CONSULTATIVE COMMITTEE - HOME AFFAIRS

13-E, Feroz Shah Road, New Delhi - 110 001

Dr. THOL.THIRUMAAVALAVAN, Ph.D

To,

Mr. K. K. Venugopal,
Attorney-General for India,
Supreme Court Complex,
New Delhi-110201.

("You")

By E-mail

Dear Sir,

Subject: Seeking Consent In Writing to initiate proceedings for Criminal Contempt under Article 129 of the Constitution of India read with S.15 of Contempt of Courts Act, 1971 read with Rule 3(c) of Rules to Regulate Proceedings for Contempt of the Supreme Court of India, 1975

1. The undersigned is a Member of Parliament, elected to the House of the People from the constituency of Chidambaram. I am also the President of the **Viduthalai Ciruthaigal Katchi**, a political party registered with the Election Commission of India. By way of this letter, I seek your consent in writing for initiating proceedings of criminal contempt under Article 129 of the Constitution of India read with Sections 15, 2(c) of the Contempt of Courts Act, 1971 and Rule 3(c) of the Rules to Regulate Proceedings for Contempt of the Supreme Court of India, 1975, against the directors of the NSO Group, an Israel based cyber weapons development company and the incumbent secretary of Home Mr.Ajay Bhalla, as well as the previous Secretary of Home Mr. Rajiv Gauba ("Alleged Contemnors / Contemnors").

2. The undersigned has been constrained, in his capacity as a citizen of this country, and as a popularly elected MP sworn to the Constitution, to seek consent for initiating contempt proceedings against the Alleged Contemnors. It has now become reasonably apparent that they were involved in an effort of military grade surveillance against a Supreme Court justice, while he still was in office, two Supreme Court registry officials on the judicial side of the writ section, and another Supreme Court staffer. This effort may have been using a spyware called *Pegasus*. This is tantamount to shockingly gross interference and obstruction of the administration of justice, for which accountability ought to be fixed *inter alia* under S.2(c)(iii) of the Contempt of Courts Act, 1971.

BACKGROUND FACTS

3. On July 18, 2021, a media consortium comprising of *The Wire*, a media organisation based in India, *Forbidden Stories,* a non-profit media organisation based in Paris, and 15 other media organisations from across the world, revealed a list of names of people who were either persons of interest, i.e. probable/potential targets, or were forensically confirmed as having been targeted for surveillance through a deadly spyware called Pegasus Spyware, developed and sold by an Israel based company known as NSO Group Technologies. *(a true copy of the Article published by The Wire is annexed as* ***Annexure-A1****)*. NSO Group, its directors and officials shall be made parties as Contemnors in the proposed Contempt Petition.

4. *Pegasus* Spyware not only allows for a deep, and extensive surveillance of the contents and communication using the infected phone – but also enables remote control of it and all its contents and functions, including access to otherwise encrypted communication. It is reported that it is also capable of remote

activation of the infected phone's camera/s and microphone, thus allowing record and relay of private conversations and meetings.

5. The list of confirmed targets revealed by the media consortium was corroborated by *Amnesty International's Security Lab* after performing in-depth forensic analysis of numerous mobile phone devices from human rights defenders (HRDs) and journalists around the world. *(a true copy of the report published by Amnesty International is annexed as* ***Annexure-A2*** *)*
6. Earlier also, in 2019, an article in the *Indian Express* had revealed that Journalists and Human Rights Activists in India have been targets of surveillance using Israeli Spyware, Pegasus. *(a true copy of the news article published by The Indian Express is annexed as* ***Annexure-A3****)*
7. It is important to note that in 2019, *Whatsapp* had itself independently found and disclosed that Pegasus was being used on those phone numbers. Some of the names on the present list of targets of Pegasus Spyware, are the same as the names that had gone out public about being notified by Whatsapp, in 2019, that their phones were targeted by the Spyware. This corroborates the current findings of the Media Consortium and Amnesty International. *(a true copy of the Article published by The Wire is annexed as* ***Annexure-A4****)*
8. Apart from this, in 2018, *Citizen Lab,* an independent entity associated with Toronto University, had published a comprehensive study identifying 45 countries, including India, in which operators of the spyware may be conducting operations. *(a true copy of the Report published by Citizen Lab is annexed as* ***Annexure-A5****)*
9. In the present case, *Amnesty International's Security Lab* submitted a sample of their forensic evidence and their general forensic methodology to independent peer review by Citizen Lab. The Citizen Lab independently validated that Amnesty International's forensic methodology correctly identified infections with NSOs

Pegasus Spyware, further corroborating the findings. Additionally, Citizen Lab's own research has also independently arrived at a number of the same key findings as Amnesty International's analysis. *(a true copy of the Report published by Citizen Lab is annexed as **Annexure-A6**)*

10. Further, *France's national cybersecurity authorities (ANSSI)* also confirmed Amnesty International's technical findings of presence of the spyware on the phone of two journalists from *Mediapart,* the country's online investigative journal. This is the further corroboration of Amnesty's findings by a government agency.
11. From the global list of 50,000 potential targets, at least 300 have been confirmed to be in India. *(a true copy of the Article published by The India Forum is annexed as **Annexure-A7**)*. The targets in India have thus far ranged from journalists to political opponents, ministers, businessmen, human rights defenders to a dissident election commissioner.
12. The NSO Group Technologies has repeatedly said that it sells the spyware **only** to vetted sovereign governments. If this is taken to be true on face value, the law of the land authorises only the Ministry of Home Affairs to organise interception of messages only in exceptional cases.
13. On several occasions the Indian government has been questioned on the use of Pegasus and the responses have been equivocal and vague. The following paras recount some of Government of India's reactions to the reportage.
14. When the Pegasus Issue was raised in the parliament on 19.08.2021, Mr. Ashwini Vaishnav, the Minister for Communications, Electronics & Information Technology and Railways, rejected report's about the use of Pegasus Spyware on Journalist, judges, and opposition leaders. He then gave this statement in the parliament:

> "*In India there is a well-established procedure through which lawful interception of electronic communication is carried out in order for the purpose of national security,*

particularly on the occurrence of any public emergency or in the interest of public safety, by agencies at the Centre and States," the government added. "The requests for these lawful interceptions of electronic communication are made as per relevant rules under the provisions of section 5(2) of Indian Telegraph Act ,1885 and section 69 of the Information Technology (Amendment) Act, 2000."

15. On 11.12.2019, in response to unstarred Question No. 3686, which was asked in the Lok Sabha by Shri Anumula Revanth Reddy, the Hon'ble Minister for Electronics & Information Technology gave the following response:

> "*Government had been informed by WhatsApp, this spyware was developed by an Israel based company NSO Group and that it had developed and used Pegasus spyware to attempt to reach mobile phones of a possible number of 1400 users globally that includes 121 users from India. Some statements have appeared based on reports in the media, regarding breach of privacy of Government had been informed by WhatsApp of a vulnerability affecting some The Government is committed to protect the fundamental rights of citizens, including the right to privacy. The Government of India for the reported breach is completely misleading. The Government operates strictly as per provisions of law and laid down protocols. There are adequate safeguards to ensure that no innocent citizen is harassed or his privacy breached*"

16. On 28.11.2019, Shri Ravi Shankar Prasad, the then Minister for Electronics and Information Technology and Communications while being questioned on the Pegasus Scandal in the Rajya Sabha, gave an equivocating response. When he was asked whether the Government of India had used the Pegasus Spyware, the Minister Answered *:"no unauthorized interception has been done, to the best of my knowledge*". And when he was Asked whether there had been any transaction between the Government and NSO group, the minister Answered : "*I have very*

specifically stated that the security agencies responsible follow a particular procedure. If there is any violation of a particular procedure, we take action, tough action and also impose a penalty."

17. Under the rules under the Telegraph Act and the Information Technology Act as cited by the Government of India, the competent authority to direct interception, monitoring or decryption is the Secretary of Home Affairs. Some of the alleged hacking and surveillance has occurred during the tenure of the present Home Secretary Mr. Ajay Bhalla and some of it in the tenure of Mr. Rajiv Gauba, the then Home Secretary (who now happens to be the Cabinet Secretary). It is therefore proposed that both Mr. Bhalla and Mr. Gauba be arraigned as Alleged Contemnors in the proposed contempt petition for which Your consent is sought. The undersigned may on the directions of Hon'ble Court or otherwise choose to arraign other government officials or other persons upon further revelations or enquiries, and/or depending on the testimony of the parties arraigned as contemnors in the first instance. Your consent sought here is on the subject matter of the alleged placing of a sitting supreme court judge, the officials of the registry and the staff under a military grade surveillance system in general and without prejudice or specificity as to the identity of the alleged contemnors.
18. On the other hand, the position taken by the NSO group on Pegasus spyware in its public utterances is as follows:

- On sale of Pegasus: NSO has maintained that it only sells the surveillance software to sovereign governments and its authorised agencies.
- On modus operandi: NSO has maintained that it "*does not operate the systems that it sells to vetted governments Bodies, and does not have access to the data of its customers' targets". (a true copy of the Article published by The Ifex is annexed as* ***Annexure-A8****)*

SUPREME COURT JUDGE AND STAFFERS TARGETED

19. Recently, the names of a former judge of the Supreme Court, Justice Arun Mishra and two former officials of the Supreme Court Registry, N.K. Gandhi and T.I. Rajput have appeared on the list of potential targets. *(a true copy of the Article published by The Indian Express is annexed as* ***Annexure-A9****)*.
20. Justice (Retd.) Arun Mishra has said on record that he had surrendered the targeted phone number in 2014, which was added to the database in 2019. However, the fact that the number which was registered in his name was added to the target list in 2019, when he was a sitting judge of the Supreme Court, is reason enough for initiating contempt. *(a true copy of the Article published by The Wire is annexed as* ***Annexure-A10****)*.
21. When numbers of the above-mentioned registry officials were added to the database, they worked in the crucial 'writ' section of the Supreme Court's registry, which handles thousands of writ petitions every year, which are of direct concern to the union government. *(a true copy of the Article published by The Wire is annexed as* ***Annexure-A10****)*.
22. The list also revealed the name of a Supreme Court Staffer, who had made allegations of Sexual Harassment against the then Chief Justice of India, Ranjan Gogoi, in April 2019. It was revealed that three of her own phone numbers, along with eight other phone numbers belonging to her husband and two of his brothers were marked as potential targets of the surveillance, in the same week when her allegations against CJI were first reported. *(a true copy of the Article published by The Wire is annexed as* ***Annexure-A11****)*
23. The attempt of surveillance being carried out on a Supreme Court judge, who was in office in 2019, when his number was added to the database, and supreme

court registry officials and staffer, using a military-grade cyber weapon, which is an act of undeclared civil war, undoubtedly amounts to an act which tends to interfere and obstruct the administration of justice, thus falling under the definition of Criminal Contempt of Court under **S. 2(c)(iii)** of the **Contempt of Courts Act, 1971**.

24. The Rule of Law is the basic foundation of any democratic society. The judiciary is the guardian and protector of Rule of Law. The judiciary of India is not merely vested with the duty to resolve conflicts but also with the special and additional duty to oversee that all individuals and institutions including the executive and the legislature, act within the framework of the constitution.[1]

25. For the judiciary to perform its duties and functions effectively it is necessary to protect the authority of courts at all costs. Any unjust interference with the work of the judiciary will weaken the cornerstone of our constitutional scheme and, hence, jeopardise the rule of law and civilised life in the society. This is the sole reason that the Judiciary in India has been vested with powers to punish those who indulge in any act which tends to interfere or obstructs the judges from discharging their duties without fear or favour.[2]

26. The foundation of the judiciary is the trust and confidence of the people in its ability to deliver fearless and impartial justice. However, when targeted surveillance or hacking is carried out on its officials and indeed a sitting judicial officer, it shakes the trust of the public in the judiciary, thus weakening the very foundation of the judiciary itself. The Hon'ble Apex Court has held that in the general interest of the community, it is imperative that the authority of courts should not be imperiled in any way and there should be no unjustifiable interference in the administration of justice. Any act which may have the

---

[1] *In Re: Vinay Chandra Mishra*, (1995) 2 SCC 584.
[2] *In Re: Vinay Chandra Mishra*, (1995) 2 SCC 584.

tendency to shake the public confidence in the fairness and impartiality of the administration of justice should not be permitted.[3]

27. The judiciary has been given the power to punish for the contempt of court to protect and vindicate the right of the public so that the administration of justice is not perverted, prejudiced, obstructed or interfered with. Any deliberate interference with the discharge of such duties would amount to criminal contempt and **the courts must take serious cognizance of such conduct.**[4]

28. The Hon'ble Supreme Court has also held that the broad test to be applied in cases of criminal contempt is whether the act complained of was calculated to obstruct or had an intrinsic tendency to interfere with the course of justice and the due administration of law. Since, the present act carried by the contemnors is very much capable of shaking the faith of the public in the judiciary, it had the tendency to interfere with the course of justice and due administration of law.[5]

29. The judiciary's power to punish for contempt of court is intended to be a protection to the public whose interests would be very much affected if by the act or conduct of any party, the authority of the court is lowered and the sense of confidence which people have in the administration of justice is weakened.[6]

30. In the present case, a foreign company has set to work a spyware on the phones of a then sitting Judge ofn the Supreme Court, one of the Supreme Court's staffers and her family members; and registry officials of the Supreme Court. Thus, all the actions of the Supreme Court taken through the targets of the surveillance would be questioned in the minds of the public. The deep faith that the public has in our judiciary is due to its independence guaranteed and protected by the Constitution of India. The very act of initiating a secret

---

[3] *Prashant Bhushan & Anr., In Re..*, (2021) 1 SCC 745.
[4] *Delhi Judicial Service Association v. State of Gujarat & Ors.,* (1991) 4 SCC 406.
[5] *S. Abdul Karim v. M. Prakash & Ors.*, (1976)1 SCC 975.
[6] *Brahma Prakash Sharma & Ors. v. State of Uttar Pradesh,* AIR 1954 SC 10.

surveillance on members of the Apex Court of the Country leads to a great threat to the independence of the judiciary, thus leading to weakening of the public's faith in the working of the judiciary.

31. What should also be considered is that, in the present case it is the executive which is alleged of contempt of court. The Ministry of Home affairs, by allowing surveillance upon the members of the judiciary, has tried to weaken the public's trust in the independent functioning of the judiciary, hence made an attempt to dismantle the very fabric of democracy. Thus, it is also a case where one arm of the State has tried to fundamentally dislodge the other arm of the State, that too, the judiciary which is the central pillar of democracy.

32. The principle of Rule of Law runs through the entire fabric of the constitution, and it is the judiciary which makes the rule of law effective by keeping every organ of the state within the limits of the law, through its power of judicial review. and therefore, it is absolutely essential that the judiciary must be independent of executive pressure or influence.[7] It is necessary that the independence of the Indian Judiciary be saved from such encroachments as it is the judiciary that stands between the citizen and the State as a bulwark against executive excesses and misuse or abuse of power by the executive.[8]

33. Fearless justice is a cardinal creed of our constitution[9], and an independent judiciary is the most essential characteristic of a democratic society. The independence and integrity of the judiciary in a democratic system of government is of the highest importance and interest not only to the judges but to the citizens at large who seek redress in the last resort in courts of law against any illegal acts or the high-handed exercise of power by the executive.[10] An

---

[7] *Madras Bar Association v. Union of India*, (2014) 10 SCC 1.
[8] *Madras Bar Association v. Union of India*, (2014) 10 SCC 1.
[9] *Union of India v. Sankalchand Himatlal Sheth*, (1977) 4 SCC 193.
[10] *Supreme Court Advocates-on-Record Association and Ors. vs. Union of India*, AIR 1994 SC 268.

interference with the independent working of the judiciary of India is an interference with the functioning of Democracy of India.

34. Judicial independence is the prime necessity for Rule of Law to prevail[11] and hence, it has to be preserved as it constitutes the foundation on which rests the edifice of our democratic polity.[12]

ADDRESSING SOME CONCERNS THAT YOU MAY HAVE

35. I would be failing in my duty if I don't engage with and address some of the concerns that may have arisen in Your mind in according the consent sought herein.

    a. Bar of Limitation u/s.20 of the Contempt of Court Act, 1971: Because the petitioner acquired the knowledge of contempt only recently, when the target list was revealed and the names of the above-mentioned persons were discovered on the list, the present Contempt proceedings shall not be barred by S.20 of the Contempt of Courts Act, 1971. It is a settled principle of law that in such situations where the petitioners received the knowledge of contempt much later after its commitment, the period of limitation has to be counted from the date of knowledge.[13] Hence, the present proceedings shall not be barred by limitation.[14] Even assuming that Section 20 were to be read literally, many of the allegations are said to have occurred in the spring of 2019, the one year from thereon ended during the pandemic period. The limitation therefore has stood extended vide *suo motu* orders of the Hon'ble Supreme Court extending all periods of limitation.

---

[11] *Subhash Sharma & Ors. v. Union of India*, 1991 Supp (1) SCC 574.
[12] *S.P. Gupta v. Union of India & Ors.*, (1981) Supp SCC 87.
[13] *Pallav Sheth v. Custodian & Ors.*, (2001) 7 SCC 549.
[14] *Bank of Baroda v. Sadruddin Hasan Daya & Anr.* (2004) 1 SCC 360.

b. That the allegations involve disputed facts and perhaps complex questions of facts and law: This application is based on *prima facie* material which has now received considerable corroboration by multiple independent efforts as explained hereinabove. Based on the reply of the alleged contemnors in the first instance, more officials may need to be proceeded against. Some reports have also been discovered which state that State Governments have also been involved in the use of Pegasus Spyware for surveillance operations. However, matter of surveillance of the Supreme Court Judge, registry officials and a staffer, most of who are residents of Delhi, it is the Union Ministry of Home Affairs that exercises Jurisdiction. The response from Government of India that all surveillance requests have been duly authorised, leads to the reasonable presumption that they have undertaken all due enquiries and found no state authorities to be acting extra-territorially. Thus, for present, the proceedings ought to be initiated against the Alleged Contemnors.

c. That the matter is *sub judice*: The Contempt Jurisdiction of the Hon'ble Supreme Court operates independently and if the present contempt proceedings is instituted, the Hon'ble Court may elect to decide the same independently or to adjudicate on the same along with other questions – including the constitutionality of certain provisions of the law and actions thereunder. There is no order restraint by the Hon'ble Court on other statutory functionaries exercising their jurisdiction. With great respect, I urge you to not consider the pending petitions as fetters on your powers and functions not just under the Contempt of Courts Act, 1971

36. Sir, I also urge you to give due consideration to the consequences of not holding the Alleged Contemnors to account if indeed an attempt had been made to hack

into the personal phones of judicial officers. I ask myself, if the judges and indeed the staff of the court feel that they may be under a constant watch of a government agency and that even if it happens there will be no accountability, will they ever be able to dispense justice with independence, and without fear or favour? Even if they do, will their functioning be reasonably seen to be independent? These are questions, I am sure You have too.

37. As the leader of the bar and being among the judiciary's wisest counsel it has ever had, I express hope and faith that You will discharge your solemn duty, not only the statutory duty under the Contempt of Courts Act, but indeed as the Attorney-General *for India* to ensure that persons (including governments) that pollute the stream of justice by assaulting the independence of the judiciary as is the case in the *Pegasus* matter are strictly held to account.

38. **For these reasons, I request you to give consent in writing to initiate the proceedings for Criminal Contempt against the Alleged Contemnors at the first instance namely the NSO Group and all the directors thereof; the present Secretary to the Government of India at the Ministry of Home Affairs, Mr. Ajay Bhalla and the previous such Secretary Mr. Rajiv Gauba. Needless to say, in the event that you do not wish to accord the consent sought for herein, I am sure that you will communicate the reasons therefor consistent with our best constitutionalist traditions.**

Thanking You

(Dr. Thol. Thirumavalavan).

New Delhi
13.08.2021