A-2

IN THE SUPREME COURT OF INDIA

CIVIL ORIGINAL JURISDICTION

PUBLIC INTEREST LITIGATION

WRIT PETITION CIVIL NO. _____ OF 2021

IN THE MATTER OF:

N. Ram & Anr. **... Petitioners**

Versus

Union of India & Ors. **... Respondents**

AND WITH

I. A. No. _____ OF 2021

An application on behalf of the petitioner/applicant for exemption from filing notarised affidavit

FOR INDEX

KINDLY SEE INSIDE PAPER-BOOK

Advocate for the Petitioners: Mr. Shadan Farasat

RECORD OF PROCEEDINGS

DATES	RECORD OF PROCEEDINGS

SYNOPSIS

This petition under Article 32 of the Constitution of India has been filed seeking urgent directions by way of a writ of mandamus or any other appropriate writ to the Respondents to disclose whether the Government of India or any of its agencies have obtained license for/used the Pegasus spyware either directly or indirectly to carry out surveillance on Indian citizens. The Petitioners are also praying for the constitution of an independent inquiry headed by a sitting or retired judge of this Hon'ble Court to probe into allegations that illegal surveillance has been carried out on *inter alia* journalists, lawyers, government ministers, opposition politicians and civil society activists using the Pegasus spyware, and consequent directions in terms of the report/recommendations of the independent inquiry.

A global investigation involving several leading publications around the world (including *inter alia* The Guardian (UK), Le Monde and Radio France (France), The Washington Post and Frontline (USA), Haaretz (Israel) and the Wire (India)) has revealed that more than 142 (one hundred and forty-two) persons, including journalists, lawyers, government ministers, opposition politicians, constitutional functionaries and civil society activists from India have been identified as potential targets for surveillance using Pegasus software. The list includes, *inter alia*:

i. Siddharth Varadarajan, founding Editor of the Wire and former Editor of the Hindu;

ii. M.K. Venu, founding Editor of the Wire;

iii. Sushant Singh, former Indian Express journalist;

iv. Paranjoy Guha Thakurta, former Editor of the Economic and Political Weekly;

v. Gagandeep Kang, a leading virologist involved in research into the Nipah virus;

vi. Rahul Gandhi, erstwhile President of the Indian National Congress;

vii. Ashwini Vaishnaw, Union Cabinet Minister for Railways, Communication, Electronics and Information Technology;

viii. Prahlad Singh Patel, Union Minister-of-State for Jal Shakti;

ix. G. Parameshwara, former Deputy Chief Minister of Karnataka;

x. Ashok Lavasa, former Election Commissioner of India; and

xi. Abhishek Banerjee, Member of Parliament for the Trinamool Congress.

The Pegasus software is a weapons grade spyware/surveillance tool manufactured by an Israeli cyber-arms firm NSO Group Technologies Limited ("**NSO Group**"). It is extremely advanced and is capable of infecting a mobile phone/ device without any interaction with the owner (also known as a zero-click attack). It can conduct extremely intrusive surveillance including *inter alia* tracking and recording calls, reading text and Whatsapp messages, collecting passwords, reading emails, accessing photos and videos, activating camera and microphone and enabling them to record events, and harvesting information from apps. It can be installed as simply as by placing a call on the targeted device, even if the call is not picked up. The NSO Group

D

claims to sell its products including Pegasus only to vetted governments to fight "crime and terror".

A forensic analysis of several mobile phones belonging to persons targeted for surveillance by the Security Lab of Amnesty International have confirmed Pegasus-induced security breaches.

These circumstances give rise to several serious questions, including *inter alia*:

a. Has targeted surveillance been conducted on journalists doctors, lawyers, opposition politicians, ministers, constitutional functionaries and civil society activists by illegally hacking into their phones using the Pegasus spyware?

b. What are the implications of such a hack? Do they represent an attempt by agencies and organisations to muzzle and chill the exercise of free speech and expression of dissent in India?

Such mass surveillance using a military-grade spyware abridges several fundamental rights and appears to represent an attempt to infiltrate, attack and destabilise independent institutions that act as critical pillars of our democratic set-up. It is also concerning to note that the the Respondents have not categorically ruled out obtaining Pegasus licenses to conduct surveillance in their response, and have taken no steps to ensure a credible and independent investigation into these extremely serious allegations.

Hence, the present petition has been preferred on *inter alia* the following grounds:

Firstly, that such targeted surveillance using military-grade spyware is an unacceptable violation of the right to privacy which has been held to be a fundamental right under Articles 14, 19 and 21 by this Hon'ble Court in **K.S. Puttaswamy v. Union of India (2017) 10 SCC 1**. The Pegasus hack is a direct attack on communicational, intellectual and informational privacy, and critically endangers the meaningful exercise of privacy in these contexts. The right to privacy extends to use and control over one's mobile phone/electronic device and any interception by means of hacking/tapping is an infraction of Article 21 (see **Para 17,18,19, PUCL v. Union of India (1997) 1 SCC 301**). Further, the use of the Pegasus spyware to conduct surveillance represents a grossly disproportionate invasion of the right to privacy.

Secondly, such targeted hacking/interception of *inter alia* journalists, doctors, lawyers, civil society activists, government ministers and opposition politicians seriously compromises the effective exercise of the fundamental right to free speech and expression under Article 19(1)(a). It has an obvious chilling effect on expression by threatening invasion into the most core and private aspects of a person's life (see **Para 21, Tehseen Poonawala vs Union of India (2018) 9 SCC 501**). The specific targeting of scores of journalists is an attack on the freedom of the press, and seriously abridges the right to know, which is an essential component of the right to free speech and expression (see **Para 32, 68; Indian Express Newspapers (Bombay) (P) Ltd. v. Union of India, (1985) 1 SCC 641**).

Thirdly, that the legal regime for surveillance under Section 5(2) of the Telegraph Act has been completely bypassed in the present case. Surveillance/interception is justified **only** in cases

F

of public emergency or in the interests of public safety, and the existence of such conditions must be inferred reasonably and cannot be determined solely on the assessment of the government (see **Para 28, PUCL v. Union of India (supra)**). Neither of these mandatory conditions have been met in the present case, rendering the surveillance wholly illegal.

Fourthly, that the hack/interception/decryption occasioned by the Pegasus spyware constitutes a criminal offence punishable under *interalia* Section 66 (computer related offences), 66B (punishment for dishonestly receiving stolen computer resource or communication device), 66E (punishment for violation of privacy) and 66F (punishment for cyberterrorism) of the IT Act, punishable with imprisonment and/or fine. The attack *prima facie* constitutes an act of cyber-terrorism that has several grave political and security ramifications, especially considering that the devices of government ministers, senior political figures and constitutional functionaries which may contain sensitive information have been targeted.

For these reasons, the present petition has been preferred.

LIST OF DATES AND EVENTS

Date	Event
2020	A list of over 50,000 (fifty thousand) mobile phone numbers belonging to targets of surveillance by clients of NSO Group was leaked to the international non-governmental organisation Amnesty International and the media non-profit Forbidden Stories. This information was

	investigated over 7 (seven) months by 17 (seventeen) reputed media organisations from around the globe, including *inter alia* The Guardian (UK), Le Monde and Radio France (France), The Washington Post and Frontline (USA), Haaretz (Israel) and the Wire (India). Whatsapp filed a suit against NSO Group, the creators of the Pegasus spyware, in the United States District Court of Northern California, for targeting the mobile phones of around 1400 users with malware. The Court dismissed NSO Group's contention that it had no role in targeting Whatsapp's users, and ruled that the case could proceed to discovery.
July, 2021	The global investigation revealed that the Pegasus software had been used by clients of NSO Group in *inter alia* India, Kazhakstan, UAE, Bahrain, Saudi Arabia, Rwanda, Hungary, Azerbaijan, Morocco and Mexico to conduct mass-scale invasive surveillance of *inter alia* politicians, human rights lawyers, activists and dissidents.
18.07.2021	It was widely reported in the media that the phones of over 100 (one hundred) Indians, including several journalists, lawyers and activists, as well as 2 sitting ministers of

	the Government of India, key opposition leaders and a former Election Commissioner of India was on the list of phone numbers accessed by the global investigation. A forensic analysis of the phones of several journalists demonstrated clear evidence of successful/attempted Pegasus-induced breaches.
19.07.2021	The Government of India responded to the media reports by issuing a cryptic statement claiming that there has been no authorized interception using Pegasus. The statement, however, is wholly bereft of any particulars and does not make any attempt at addressing the extremely grave questions raised by reports of the use of Pegasus.
20.07.2021	The NSO Group issued a statement where it refuses to categorically deny that it supplied the Pegasus software to government clients, including the Government of India.
After 20.07.2021	Despite the extremely serious nature of the allegations and the obvious impact of surveillance on the exercise of fundamental rights under Article 14, 19 and 21, no credible attempt is made by the

	Respondents to investigate the extent of the use of Pegasus spyware or the entities responsible for such use.
26.07.2021	Hence, the present petition.

IN THE SUPREME COURT OF INDIA

CIVIL ORIGINAL JURISDICTION

PUBLIC INTEREST LITIGATION

WRIT PETITION CIVIL NO. _____ OF 2021

(Petition under Article 32 of The Constitution of India for issuance of writ in the nature of mandamus or any other appropriate writ**)**

In the matter of:

1. N. Ram, S/o [redacted], aged about [redacted] years, R/o [redacted], email address is [redacted] and mobile number is [redacted] – Taxable

… Petitioner No. 1

2. Sashi Kumar Balakrishnan Menon, S/o [redacted], aged about [redacted] years, R/o [redacted], email address is [redacted] and mobile number is [redacted] – Taxable … **Petitioner No. 2**

Versus

1. Union of India, Ministry of Home Affairs, through the Secretary, North Block, New Delhi-110001.

2. Union of India, Ministry of Electronics and Information Technology, through the Secretary, Electronics Niketan, 6, CGO Complex, Lodhi Road, New Delhi-110001.

3. Union of India, Ministry of Communications through the Secretary, Sanchar Bhawan, 20, Ashoka Road, New Delhi-110001. … **Respondents**

All respondents are contesting respondents.

PETITION UNDER ARTICLE 32 OF THE CONSTITUTION OF INDIA FOR ISSUANCE OF WRIT IN

THE NATURE OF MANDAMUS OR ANY OTHER APPROPRIATE WRIT

To

The Hon'ble the Chief Justice of India

and his companion Justices of

the Supreme Court of India.

The humble petition

of the Petitioner above named

MOST RESPECTFULLY SHOWETH:

1. The Petitioners have approached this Hon'ble Court seeking urgent directions to the Respondents by way of a writ of mandamus or any other appropriate writ to disclose whether the Government of India or any of its agencies have obtained license for/used the Pegasus software manufactured by the Israeli cyber-arms firm NSO Group Technologies Limited ("**NSO Group**") to carry out surveillance in India, as has been widely reported by the domestic and international press. The Petitioners are also praying for the constitution of an independent inquiry headed by a sitting or retired judge of this Hon'ble Court to probe into allegations that illegal surveillance has been carried out on *inter alia* journalists, doctors, lawyers, civil society activists, government ministers and opposition politicians using the Pegasus software, and consequent directions in terms of the report/recommendations of such inquiry.

2. The Petitioners respectfully submit that such targeted surveillance using the military-grade Pegasus software is an attack on fundamental rights, including the right to privacy under Articles 14, 19 and 21 and the right to free speech and

expression under Article 19(1)(a) of the Constitution. Snooping on journalists, doctors, lawyers, civil society activists, government ministers, opposition politicians and constitutional functionaries is not only illegal under the relevant legislations (the Telegraph Act, 1885 and the Information Technology Act, 2000), but is also a Nixonian attempt to infiltrate, attack and destabilise independent institutions that act as critical checks and balances in a democratic set-up.

The Petitioners

3. The Petitioner No. 1 is a citizen of India and is a journalist and editor, who has served as Editor-in-Chief, Publisher and Chairman of the Hindu Group of publications, which *inter alia* publishes the Hindu, the Hindu Business Line and Frontline. He presently serves as a Director of the Hindu Group of publications. He is a resident of Chennai, his email address is [redacted] and mobile number [redacted] The annual income of the Petitioner No. 1 is in excess of INR [redacted] and is taxable. A true copy of the [redacted] of the Petitioner No. 1 is attached herewith as **ANNEXURE P-1** at page **28**. The full name of the Petitioner No. 1, as reflected in his PAN card is Narasimhan Ram. N. Ram and Narasimhan Ram are one and the same person.

4. The Petitioner No. 2 is a citizen of India and is a print and broadcast journalist, filmmaker and media entrepreneur. He founded and chairs the Media Development Foundation which administers the Asian College of Journalism. He was among the earliest newscasters in English on national television Doordarshan and has also served as the West Asia

Correspondent for the Hindu. In 1992, he founded and launched Asianet, India's first satellite TV channel in a regional language (Malayalam), and the country's first statewide cable TV network in Kerala. He has anchored and produced numerous shows, documentaries and features for national television in India. He is a resident of Chennai, his email address is [redacted] and mobile number [redacted]. The annual income of the Petitioner No. 2 is in excess of [redacted] and is taxable. A true copy of [redacted] of the Petitioner No. 2 is attached herewith as **ANNEXURE P-2** at page **29**.

FACTUAL BACKGROUND

What is the Pegasus software?

5. The Pegasus software is a **military grade hacking spyware** manufactured by the Israeli cyber-arms manufacturing firm NSO Group that can be covertly installed on mobile phones running both Android and iOS operating systems, as well as other electronic devices.

6. The Pegasus spyware is so advanced that it can infect a device without any interaction with its owner. Normally, hacking softwares involve a malicious link that owners of the device are tricked into clicking. But Pegasus does not need the owner of the device to perform any action or click on any link for the spyware to infect the device. In fact, it could be installed by the simple mechanism of placing a call on the targeted device, even if the call is not picked up.

What can the Pegasus software do?

7. The Pegasus software is capable of extremely intrusive surveillance including *inter alia* tracking and recording

calls, reading text and Whatsapp messages, collecting passwords, reading emails, accessing photos and videos, activating camera and microphone and enabling them to record events, and harvesting information from apps.

A true copy of a chart titled "*What Pegasus spyware can do*" is annexed herewith as **ANNEXURE P-3** at page **30**.

Who can access/use Pegasus software?

8. The Pegasus software is licensed to governments around the world. The website of the NSO Group (accessible at https://www.nsogroup.com/about-us/) claims that its products, which includes the Pegasus software, are used **exclusively** by government intelligence and law enforcement agencies to fight "crime and terror". A true copy of "*About Us*" section of the website of NSO Group is annexed herewith as **ANNEXURE P-4** at pages **31** to **35**.

The "Pegasus Project": Media revelations

9. In 2020, a list of over 50,000 (fifty thousand) mobile phone numbers belonging to targets of surveillance by clients of NSO Group was leaked to the international non-governmental organisation Amnesty International and the media non-profit Forbidden Stories. This information was investigated over 7 (seven) months by 17 (seventeen) reputed media organisations from around the globe, including *inter alia* The Guardian (UK), Le Monde and Radio France (France), The Washington Post and Frontline (USA), Haaretz (Israel) and the Wire (India).

10. The consortium of media outlets discovered that the Pegasus software had been used by clients of NSO Group in India, Kazakhstan, UAE, Bahrain, Saudi Arabia, Rwanda, Hungary, Azerbaijan, Morocco and Mexico to conduct

mass-scale invasive surveillance of *inter alia* politicians, human rights lawyers, activists and dissidents. A true copy of article titled "*Pegasus Project: spyware leak suggests lawyers and activists at risk across globe*" dated 19.07.2021 published on the Guardian website is annexed herewith as **ANNEXURE P-5** at pages **36** to **46**.

11. That the global investigation has revealed that over 100 (one hundred) persons, including politicians, journalists, lawyers, professors, doctors/scientists, activists and a former Supreme Court staff member were identified as potential targets for surveillance from India. Some key names whose telephone numbers featured on the list of persons targeted for surveillance include:

i. Siddharth Varadarajan, founding Editor of the Wire and former Editor of the Hindu;

ii. M.K. Venu, founding Editor of the Wire;

iii. Sushant Singh, former Indian Express journalist;

iv. Paranjoy Guha Thakurta, former Editor of the Economic and Political Weekly;

v. Gagandeep Kang, a leading virologist involved in research into the Nipah virus;

vi. Rahul Gandhi, erstwhile President of the Indian National Congress;

vii. Ashwini Vaishnaw, Union Cabinet Minister for Railways, Communication, Electronics and Information Technology;

viii. Prahlad Singh Patel, Union Minister-of-State for Jal Shakti;

ix. G. Parameshwara, former Deputy Chief Minister of Karnataka;

x. Ashok Lavasa, former Election Commissioner of India; and

xi. Abhishek Banerjee, Member of Parliament for the Trinamool Congress.

The list of 142 persons also includes a former employee of this Hon'ble Court and several members of her family.

A true copy of article titled "*Pegasus Project: 142 names revealed by the Wire on Snoop List So Far*" dated 26.07.2021 published on the Wire is annexed hereto as **ANNEXURE P-6** at pages **47** to **67**. A true copy of article titled "*Phones of 2 Ministers, 3 Opp Leaders among many targeted for surveillance*" dated 19.07.2021 published on the Indian Express website is annexed hereto as **ANNEXURE P-7** at pages **68** to **72**. A true copy of article titled "*Express journalists among over 40 whose numbers on target list*" dated 19.07.2021 published on the Indian Express website is annexed hereto as **ANNEXURE P-8** at pages **73** to **76**.

12. A forensic analysis of mobile phones of several journalists on the list by Amnesty International's Security Lab showed that the owners of the devices were all either victims of an attempted hack or a successful compromise. A true copy of article titled "*Snoop List has 40 Indian Journalists, Forensic Tests Confirm Presence of Pegasus Spyware on Some*" dated 18.07.2021 published on the Wire is annexed hereto as **ANNEXURE P-9** at pages **77** to **90**.

13. The methodology used by Amnesty International's Security Lab to identify Pegasus spyware has been validated as sound by the Citizen Lab of the Munk School of Global Affairs & Public Policy of the University of Toronto. Its

own research also led it to arrive at the same findings as Amnesty International. A true copy of report titled "*Independent Peer Review of Amnesty International's Forensic Methods for identifying Pegasus Spyware*" dated 18.07.2021 published by the Citizen Lab of the Munk School of Global Affairs & Public Policy of the University of Toronto is annexed hereto as **ANNEXURE P-10** at pages **91** to **94**. A true copy of article titled "*Canadian lab says Amnesty's technique in digging up Pegasus hack is 'sound'*" dated 19.07.2021 published on the Hindustan Times website is annexed hereto as **ANNEXURE P-11** at pages **95** to **96**.

Whatsapp and the NSO Group

14. It is also pertinent to note that the NSO Group, the creators of the Pegasus software, had been sued in the United States District Court of Northern California by Whatsapp Inc., which accused the company of targeting the mobile phones of 1400 (one thousand and four hundred) users including more than a dozen journalists from India with malware. The NSO Group argued that it had no role in targeting Whatsapp's users. However, this contention was dismissed by the learned Judge who allowed the case to proceed to discovery and held:

> "*To rebut those allegations, defendants offer the declaration of Shalev Hulio, NSO's CEO and co-founder, wherein he declares that "NSO markets and licenses the Pegasus technology to its sovereign customers, which then operate the technology themselves . . . ." Hulio Decl. ¶ 14. "Defendants role is limited to NSO providing advice and technical support to assist customers in setting up—not operating—the Pegasus technology." Id. Two points limit the persuasiveness of the declaration. First, the declaration itself leaves open the possibility of defendants' involvement in the intentional act because Hulio qualifies his statement on defendants' limited advice and technical support role by stating* ***"[w]hen Defendants provide those support services, they do so entirely at the direction of***

> ***their government customers, and Defendants follow those directions completely." Id. Thus, it appears defendants retained some role in conducting the intentional act, even if it was at the direction of their customers****..."*
>
> (emphasis supplied)

A true copy of article titled "*US Judge: Whatsapp lawsuit against Israeli spyware firm NSO can proceed*" dated 17.07.2020 published on the Guardian website is annexed hereto as **ANNEXURE P-12** at pages **97** to **99**. A true copy of judgment dated 16.07.2020 in Case No. 19-cv-07123-PJH passed by the District Court of Northern California titled **Whatsapp Inc. et al v. NSO Group Technologies Limited et al** is annexed hereto as **ANNEXURE P-13** at pages **100** to **144**.

Response by Government of India and NSO Group

15. The Respondents have issued a cryptic statement on 19.07.2021 claiming that there has been no unauthorised interception using Pegasus. However, the statement of the Respondents is wholly bereft of particulars and makes no attempt at addressing any question raised by *inter alia* the above cited media reports, including but not limited to forensic audits confirming Pegasus-induced security breaches. A true copy of "*Government Response On Pegasus Controversy: Full Statement*" dated 19.07.2021 as reported on the NDTV website is annexed hereto as **ANNEXURE P-14** at pages **145** to **147**.

16. NSO Group has also issued a statement to the Guardian through its counsel. Its response states that it supplies its products to "vetted" foreign governments and does not categorically deny that it supplied the Pegasus software to government clients, including the Government of India, in

the first place. A true copy of article titled "*Response from NSO and governments*" dated 20.07.2021 published on the Guardian website is annexed hereto as **ANNEXURE P-15** at pages **148** to **152**.

17. The present circumstances raise several important questions, which include *inter alia*:

a. Has targeted surveillance been conducted on journalists, doctors/scientists, lawyers, opposition politicians, ministers, constitutional functionaries and civil society activists by illegally hacking into their phones using the Pegasus spyware ?

b. What are the implications of such a hack? Do they represent an attempt to muzzle and chill the exercise of free speech and expression of dissent in India?

18. The Respondents have made absolutely no attempt to conduct any credible investigation into these extremely concerning allegations of mass surveillance, which have far-reaching consequences for *inter alia* the exercise of the right to free speech and expression under Article 19(1)(a) and the right to privacy under Articles 14, 19 and 21.

19. Hence, being left with no alternative, the Petitioners are constrained to approach this Hon'ble Court on *inter alia* the following grounds:

GROUNDS

A. That such targeted surveillance using weapons grade Pegasus software violates Article 21, 19 and 14 of the Constitution of India, as it breaches the right to privacy and the right to freedom of speech and expression. The present surveillance is also in complete derogation of the Telegraph

Act, 1885 and the Information Technology Act, 2000 and as such is completely illegal and a criminal act.

Right to privacy

B. That such targeted surveillance violates the right to privacy, which is the constitutional core of human dignity and is protected under Article 21, 19, 14, 25, 28, the Preamble and Part III of the Constitution according to the landmark judgment of a nine-judge bench of this Hon'ble Court in **K.S. Puttaswamy v. Union of India (2017) 10 SCC 1**.

C. That communicational, intellectual and informational privacy form essential components of an individual's right to privacy (see **Para 249, 250; K.S. Puttaswamy (supra)**). Hacking/interception, such as in the present case, critically endangers the meaningful exercise of the right to privacy in these contexts.

D. That the right to privacy extends to the use and control over one's mobile phone, including but not limited to both oral conversations and messages, and any interception by means of tapping/hacking is a breach of privacy and an infraction of Article 21 of the Constitution.

E. That this Hon'ble Court has held in **PUCL v. Union of India (1997) 1 SCC 301, at page 311 :**

> "***17.*** *We have, therefore, no hesitation in holding that right to privacy is a part of the right to "life" and "personal liberty" enshrined under Article 21 of the Constitution. Once the facts in a given case constitute a right to privacy, Article 21 is attracted. The said right cannot be curtailed "except according to procedure established by law".*
> ***18.*** *The right to privacy — by itself — has not been identified under the Constitution. As a concept it may be too broad and moralistic to define it judicially. Whether right to privacy can be claimed or has been infringed in a given case would depend on the facts of the said case. <u>But the right to hold a telephone conversation in the privacy of one's home or office without interference can certainly be claimed as "right to privacy". Conversations on the</u>*

> *telephone are often of an intimate and confidential character. Telephone conversation is a part of modern man's life. It is considered so important that more and more people are carrying mobile telephone instruments in their pockets. Telephone conversation is an important facet of a man's private life. Right to privacy would certainly include telephone conversation in the privacy of one's home or office. Telephone-tapping would, thus, infract Article 21 of the Constitution of India unless it is permitted under the procedure established by law.*
>
> ***19.*** *Right to freedom of speech and expression is guaranteed under Article 19(1)(a) of the Constitution. This freedom means the right to express one's convictions and opinions freely by word of mouth, writing, printing, picture, or in any other manner. When a person is talking on telephone, he is exercising his right to freedom of speech and expression. Telephone-tapping unless it comes within the grounds of restrictions under Article 19(2) would infract Article 19(1)(a) of the Constitution*."
>
> (emphasis supplied)

The above observations of a 2-Judge Bench of this Hon'ble Court have also been endorsed by a 9-Judge Bench in **K.S. Puttaswamy (supra)** at **Para 69, 70, 373, 512**.

F. That the nature of surveillance occasioned by the Pegasus spyware completely fails the test of proportionality, rendering the restraints it places on the right to privacy completely unjustifiable (see **Para 310, 325, K.S. Puttswamy (supra)**). It is settled law that for any invasion of privacy to be justifiable, the following conditions must be satisfied:

a. A legitimate State aim;

b. A rational nexus between the aim and the infringement of the right (the rationality prong);

c. The infringement must be the least restrictive measure available (i.e., alternatives must be unquestionably foreclosed) (the necessity prong); and

d. There must be a balance between the extent of the restrictions and the benefit the State hopes to achieve (proportionality *stricto sensu)*.

G. That not a single prong of the four-step proportionality test has been met in the present case. No legitimate State aim can be inferred from the mass surveillance of *inter alia* journalists, doctors, lawyers, civil society activists, government ministers and opposition politicians. In the absence of such an aim, there cannot exist any rational nexus between it and the invasion of privacy occasioned by the software in the present case. Snooping using a weapons-grade software sold by an Israeli cyber-arms firm can by no means be considered the least restrictive measure available. Lastly, not only can legitimate benefit be inferred from the such mass surveillance, but the same causes active harm to a democratic polity.

Right to freedom of speech and expression

H. That the conscious targeting of politically engaged persons such as journalists, doctors, lawyers, civil society activists, government ministers, opposition politicians and constitutional functionaries for surveillance seriously compromises the effective exercise of the fundamental right to free speech and expression under Article 19(1)(a).

I. That the mere fact that such a software has been used on so many mobile phones/electronic devices of politically engaged persons is likely to create a perception that those who "speak out" are at risk of being placed under surveillance using weapons grade spyware. This threatens dissenters against exercising their right to free speech and expression by means of an imminent extra-legal threat of

surveillance into the most core and private aspects of their person. This has a definite "chilling effect" on freedom of speech and expression, and silences legitimate dissent.

J. That the impact of a "chilling effect" in an extra-legal context has been recognised by this Hon'ble Court in **Tehseen Poonawala vs Union of India (2018) 9 SCC 501:**

> "21. *Freedom of speech and expression is the elan vital of sustenance of all other rights and is the very seed for germinating the growth of democratic views. Plurality of voices celebrates the constitutionalist idea of a liberal democracy and ought not to be suppressed. Pluralism and tolerance are essential virtues and constitute the building blocks of a truly free and democratic society.* ***It must be emphatically stated that a dynamic contemporary constitutional democracy imbibes the essential feature of accommodating pluralism in thought and approach so as to preserve cohesiveness and unity. Intolerance arising out of a dogmatic mindset sows the seeds of upheaval and has a chilling effect on freedom of thought and expression.*** *Hence, tolerance has to be fostered and practised and not allowed to be diluted in any manner."*

(emphasis supplied)

K. That the targeted surveillance and harvesting of personal data of several prominent journalists represents an attack on the press, which is the fourth pillar of democracy and plays a vital role as an accountability mechanism in a democratic set-up. The hacks/surveillance occasioned by Pegasus pose a real risk of compromising the ability of the press to function freely. It is a settled position of law that the right to free speech and expression includes freedom of the press within its ambit, and any interference with the same is contrary to the constitutional mandate. This Hon'ble Court has held in **Indian Express Newspapers (Bombay) (P) Ltd. v. Union of India, (1985) 1 SCC 641 at page 664**:

> "***32.*** *In today's free world freedom of press is the heart of social and political intercourse. The press has now assumed the role of the public educator making formal and non-formal education possible in a large scale*

particularly in the developing world, where television and other kinds of modern communication are not still available for all sections of society. The purpose of the press is to advance the public interest by publishing facts and opinions without which a democratic electorate cannot make responsible judgments. Newspapers being purveyors of news and views having a bearing on public administration very often carry material which would not be palatable to Governments and other authorities. The authors of the articles which are published in newspapers have to be critical of the actions of Government in order to expose its weaknesses. Such articles tend to become an irritant or even a threat to power. Governments naturally take recourse to suppress newspapers publishing such articles in different ways. Over the years, Governments in different parts of the world have used diverse methods to keep press under control. They have followed carrot-and-stick methods. Secret payments of money, open monetary grants and subventions, grants of lands, postal concessions, Government advertisements, conferment of titles on editors and proprietors of newspapers, inclusion of press barons in cabinet and inner political councils etc. constitute one method of influencing the press. The other kind of pressure is one of using force against the press. Enactment of laws providing for pre-censorship, seizures, interference with the transit of newspapers and demanding security deposit, imposition of restriction on the price of newspapers, on the number of pages of newspapers and the area that can be devoted for advertisements, withholding of Government advertisements, increase of postal rates, imposition of taxes on newsprint, canalisation of import of newsprint with the object of making it unjustly costlier etc. are some of the ways in which Governments have tried to interfere with freedom of press. ***It is with a view to checking such malpractices which interfere with free flow of information, democratic constitutions all over the world have made provisions guaranteeing the freedom of speech and expression laying down the limits of interference with it. It is, therefore, the primary duty of all the national courts to uphold the said freedom and invalidate all laws or administrative actions which interfere with it, contrary to the constitutional mandate.***"

(emphasis supplied)

L. That the targeted surveillance of journalists has a direct and demonstrable impact on the "right to know" of the citizen public. The press plays a vital role in keeping citizens informed and is critical to enabling public participation in

administration and governance and surveillance of this nature severely retards the quality and content of journalism. It is a settled constitutional position that the right to know is an extension of the right to free speech and expression under Article 19(1)(a) (see **Para 16, Dinesh Trivedi v. Union of India (1997) 4 SCC 306**; **Para 29.1-Para 29.2, Resurgence India v. Election Commission of India & Anr. (2014) 14 SCC 189**). The critical importance of the exercise of this right in the context of public affairs has been discussed by this Hon'ble Court in **Indian Express Newspapers (Bombay) (P) Ltd. (supra) at page 685:**

> "***68.*** *We have carefully considered the above two decisions. In the first case the Court was concerned with the newspaper price-page policy and in the second the newsprint policy imposed by the Government had been challenged. Neither of them was concerned with the power of Parliament to levy tax on any goods used by the newspaper industry. As we have observed earlier taxes have to be levied for the support of the Government and newspapers which derive benefit from the public expenditure cannot disclaim their liability to contribute a fair and reasonable amount to the public exchequer. What may, however, have to be observed in levying a tax on newspaper industry is that it should not be an over-burden on newspapers which constitute the Fourth Estate of the country. Nor should it single out newspaper industry for harsh treatment. A wise administrator should realise that the imposition of a tax like the customs duty on newsprint is an imposition of knowledge and would virtually amount to a burden imposed on a man for being literate and for being conscious of his duty as a citizen to inform himself about the world around him. "**The public interest in freedom of discussion (of which the freedom of the press is one aspect) stems from the requirement that members of a democratic society should be sufficiently informed that they may influence intelligently the decisions which may affect themselves." (Per Lord Simon of Glaisdale in Attorney-General v. Times Newspapers Ltd. [(1973) 3 All ER 54 : 1974 AC 273 : (1973) 3 WLR 298 (HL)]). Freedom of expression, as learned writers have observed, has four broad social purposes to serve: (i) it helps an individual to attain self fulfilment, (ii) it assists in the***

> ***discovery of truth, (iii) it strengthens the capacity of an individual in participating in decision-making and (iv) it provides a mechanism by which it would be possible to establish a reasonable balance between stability and social change. All members of society should be able to form their own beliefs and communicate them freely to others. In sum, the fundamental principle involved here is the people's right to know. Freedom of speech and expression should, therefore, receive a generous support from all those who believe in the participation of people in the administration****. It is on account of this special interest which society has in the freedom of speech and expression that the approach of the Government should be more cautious while levying taxes on matters concerning newspaper industry than while levying taxes on other matters. It is true that this Court has adopted a liberal approach while dealing with fiscal measures and has upheld different kinds of taxes levied on property, business, trade and industry as they were found to be in the public interest. But in the cases before us the Court is called upon to reconcile the social interest involved in the freedom of speech and expression with the public interest involved in the fiscal levies imposed by the Government specially because newsprint constitutes the body, if expression happens to be the soul.*"
>
> (emphasis supplied)

Legal regime for surveillance

M. That the legal regime for surveillance in India under the Telegraph Act, 1885 ("**Telegraph Act**") and the Information Technology Act, 2000 ("**IT Act**") have been completely bypassed in the present case, rendering the surveillance through Pegasus not just illegal, but criminal.

The Telegraph Act, 1885

N. That Section 5(2) of the Telegraph Act states:

> "(2) On the occurrence of any **public emergency**, or in the interest of the **public safety**, the Central Government or a State Government or any officer specially authorised in this behalf by the Central Government or a State Government may**, if satisfied that it is necessary or expedient so to do in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of an offenc**e, for reasons to be recorded in writing, by order, direct that any message or class of messages to or from any person or

> class of persons, or relating to any particular subject, brought for transmission by or transmitted or received by any telegraph, shall not be transmitted, or shall be intercepted or detained, or shall be disclosed to the Government making the order or an officer thereof mentioned in the order:
> Provided that press messages intended to be published in India of correspondents accredited to the Central Government or a State Government shall not be intercepted or detained, unless their transmission has been prohibited under this sub-section."

(emphasis supplied)

O. That none of the above necessary conditions for resorting to interception have been met in the present case. The targets of interception here are reputed journalists, doctors, lawyers, civil society activists, government ministers and opposition politicians. There is evidently no threat posed by them to the sovereignty or integrity of India, the security of the state, friendly relations with foreign states, public order or incitement to an offence. Neither is there any public emergency or issue of public safety involved. None of the mandatory conditions that need to exist prior to authorisation of interception/surveillance are present here. The surveillance is thus obviously illegal.

P. That in **PUCL v. Union of India (supra)**, this Hon'ble Court held that there is **no** jurisdiction to exercise powers under Section 5(2) of the Telegraph if a public emergency has not occurred or the interests of public safety do not demand it. The existence of a public emergency or public safety considerations **do not** depend on the assessment of the government alone, and must be reasonably inferable:

> ***28.*** *Section 5(2) of the Act permits the interception of messages in accordance with the provisions of the said section. "Occurrence of any public emergency" or "in the interest of public safety" are the sine qua non for the application of the provisions of Section 5(2) of the Act. Unless a public emergency has occurred or the interest of public safety demands, the authorities have no jurisdiction*

> *to exercise the powers under the said section.* ***Public emergency would mean the prevailing of a sudden condition or state of affairs affecting the people at large calling for immediate action. The expression "public safety" means the state or condition of freedom from danger or risk for the people at large. When either of these two conditions are not in existence, the Central Government or a State Government or the authorised officer cannot resort to telephone-tapping even though there is satisfaction that it is necessary or expedient so to do in the interests of sovereignty and integrity of India etc. In other words, even if the Central Government is satisfied that it is necessary or expedient so to do in the interest of the sovereignty and integrity of India or the security of the State or friendly relations with sovereign States or public order or for preventing incitement to the commission of an offence, it cannot intercept the messages or resort to telephone-tapping unless a public emergency has occurred or the interest of public safety or the existence of the interest of public safety requires. Neither the occurrence of public emergency nor the interest of public safety are secretive conditions or situations. Either of the situations would be apparent to a reasonable person****.*
>
> (at page 313, emphasis supplied)

The Information Technology Act, 2000

Q. That the military-grade Pegasus software is effectively a mechanism for hacking into a mobile phone/electronic device and *inter alia* monitoring and harvesting personal data. The software is capable of monitoring and recording telephone calls, private messages, emails and location, and also turn on microphone and camera without the knowledge of the owner of the device.

R. That this is not only a gross violation of privacy, but also a criminal offence under the following provisions of the IT Act:

i. Section 66 (computer related offences), punishable with imprisonment of up to 3 (three) years or fine up to INR 5,00,000 (five lakhs) or both;

ii. 66B (punishment for dishonestly receiving stolen computer resource or communication device), punishable with imprisonment for up to three years or fine up to INR 1,00,000 (one lakh) or both;

iii. 66E (punishment for violation of privacy), punishable with imprisonment for up to 3 (three) years or fine up to INR 2,00,000 (two lakhs) or both; and

iv. 66F (punishment for cyberterrorism), punishable with imprisonment up to life.

S. That Section 66F of the IT Act states as under:

> "***66-F. Punishment for cyber terrorism***.—*(1) Whoever,—*
>
> ***(A)*** ***with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by***—
>
> ***(i)*** *denying or cause the denial of access to any person authorised to access computer resource; or*
>
> ***(ii)*** ***attempting to penetrate or access a computer resource without authorisation or exceeding authorised access****; or*
>
> ***(iii)*** ***introducing or causing to introduce any computer contaminant****,*
>
> *and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or* ***knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community*** *or adversely affect the critical information infrastructure specified under Section 70; or*
>
> ***(B)*** ***knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States,***

public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise*, commits the offence of cyber terrorism.*

(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.]

(emphasis supplied)

T. That the hack by Pegasus appears to *prima facie* constitute an of cyber-terrorism. The devices of *inter alia* government ministers, senior political figures and constitutional functionaries which may contain sensitive information have been targeted. This has wide-reaching ramifications for governance and administration in the country. It is imperative that a thorough and independent investigation be conducted to assess the source and nature of the threat posed by the Pegasus hack.

U. That the government response does not provide any clarity whatsoever on how such mass surveillance using military grade software was carried out with such impunity. This is clearly illegal and a serious abridgment of fundamental rights, not to mention a criminal offence.

V. That no investigation into these extremely serious allegations has been initiated by the Respondents, despite the extremely grave ramifications of such a targeted attack using weapons-grade spyware.

W. That it is essential to initiate a thorough, independent and effective investigation to analyse the source, method and actors involved in the Pegasus spyware attack, which has had a direct and demonstrable impact on the exercise of critical fundamental rights under Articles 14, 19 and 21 across the territory of India.

X. In these circumstances, the Petitioners have approached this Hon'ble Court under Article 32 of the Constitution of India to protect these fundamental rights. The Petitioners have no alternative remedy, much less an equally efficacious remedy. The urgent intervention of this Hon'ble Court in the form of directions to the Respondents to immediately disclose whether the Government of India or its agencies have obtained license and/or conducted surveillance using the Pegasus spyware, and the constitution of an inquiry headed by a sitting or retired judge of this Hon'ble Court to probe into these extremely serious events.

Y. That the Petitioners have not filed any other or such petition before this Hon'ble Court or any other High Court.

Z. The Petitioners reserves their right to request leave of this Hon'ble Court to add to or amend this petition at a later stage, as may be appropriate.

PRAYER

In view of the facts and circumstances stated above, it is most respectfully prayed that this Hon'ble Court may be pleased to:

a. Issue a writ/order or direction in the nature of mandamus or any other appropriate writ directing the Respondents to disclose if the Government of India or any of its agencies have obtained license(s) for Pegasus spyware and/or used/employed it, either directly or indirectly, to conduct surveillance in any manner whatsoever; and

b. Issue a writ/order or direction in the nature of mandamus or any other appropriate writ constituting an inquiry to investigate the extent of surveillance on Indian citizens using Pegasus spyware and the entities responsible for it,

headed by a sitting or retired judge of this Hon'ble Court duly nominated by this Hon'ble Court; and

c. Issue a writ/order or direction in the nature of mandamus or any other appropriate writ providing consequent relief in terms of the report/recommendation of any inquiry constituted in terms of (b) above; and/or

d. Pass any other orders/directions that may be deemed appropriate in the interest of justice.

AND FOR THIS ACT OF KINDNESS, THE PETITIONER AS IN DUTY BOUND SHALL EVER PRAY.

Filed by:

Place: New Delhi

Date: 26.07.2021



SHADAN FARASAT

Advocate for the Petitioners