1834722/2021/CL&ES

REPORTABLE

IN THE SUPREME COURT OF INDIA

CRIMINAL /CIVIL ORIGINAL JURISDICTION

WRIT PETITION (CRL.) NO. 314 OF 2021

MANOHAR LAL SHARMA …PETITIONER

VERSUS

UNION OF INDIA AND ORS. …RESPONDENT(S) With

WRIT PETITION (CIVIL) NO. 826 OF 2021

With

WRIT PETITION (CIVIL) NO. 909 OF 2021

With

WRIT PETITION (CIVIL) NO. 861 OF 2021

With

WRIT PETITION (CIVIL) NO. 849 OF 2021

With

WRIT PETITION (CIVIL) NO. 855 OF 2021

With

WRIT PETITION (CIVIL) NO. 829 OF 2021

With

WRIT PETITION (CIVIL) NO. 850 OF 2021

With

WRIT PETITION (CIVIL) NO. 848 OF 2021

With

WRIT PETITION (CIVIL) NO. 853 OF 2021

With

WRIT PETITION (CIVIL) NO. 851 OF 2021

With

WRIT PETITION (CIVIL) NO. 890 OF 2021

ORDER

The Court is convened through Video Conferencing.

"If you want to keep a secret, you must also hide it from yourself." -George Orwell, 1984 ***1.*** The present batch of Writ Petitions raise an Orwellian concern, about the alleged possibility of utilizing modern technology https://playaviatorgame.net/ to hear what you hear, see what you see and to know what you do. In this context, this Court is called upon to examine an allegation of the use of such a technology, its utility, need and alleged abuse. We make it clear that our effort is to uphold the constitutional aspirations and rule of law, without allowing ourselves to be consumed in the political rhetoric. This

Court has always been conscious of not entering the political thicket. However, at the same time, it has never cowered from protecting all from the abuses of fundamental rights. All that we would like to observe in this regard is a reiteration of what had already been said by this Court in ***Kesavananda Bharati v. State of Kerala,*** *(Opinion of Justice Khanna)* AIR 1973 SC 1461:

> "**1535**…. Judicial review is not intended to create what is sometimes called judicial oligarchy, the aristrocracy (*sic*) of the robe, covert legislation, or Judge-made law. The proper forum to fight for the wise use of the legislative authority is that of public opinion and legislative assemblies. Such contest cannot be transferred to the judicial arena. That all constitutional interpretations have political consequences should not obliterate the fact that the decision has to be arrived at in the calm and dispassionate atmosphere of the court room, that Judges in order to give legitimacy to their decision have to keep aloof from the din and controversy of politics and that the fluctuating fortunes of rival political parties can have for them only academic interest. Their primary duty is to uphold the Constitution and the laws without fear or favour and in doing so, they cannot allow any political ideology or economic theory, which may have caught their fancy, to colour the decision…"

2. A short conspectus of the events leading up to the present batch of petitions would not be misplaced to highlight the scope of the issues at hand. In September 2018, Citizen Lab, which is a laboratory based out of the University of Toronto, Canada,

released a report detailing the software capabilities of a "spyware suite" called Pegasus that was being produced by an Israeli Technology firm, *viz.*, the NSO

Group. The report indicated that individuals from nearly 45 countries were suspected to have been affected.

3. The Pegasus suite of spywares can allegedly be used to compromise the digital devices of an individual through zero click vulnerabilities, *i.e.*, without requiring any action on the part of the target of the software. Once the software infiltrates an individual's device, it allegedly has the capacity to access the entire stored data on the device, and has real time access to emails, texts, phone calls, as well as the camera and sound recording capabilities of the device. Once the device is infiltrated using Pegasus, the entire control over the device is allegedly handed over to the Pegasus user who can then remotely control all the functionalities of the device and switch different features on or off. The NSO Group purportedly sells this extremely powerful software only to certain undisclosed Governments and the end user of its products are "exclusively government intelligence and law enforcement agencies" as *per* its own website.

4. In May 2019, the global messaging giant WhatsApp Inc. identified a vulnerability in its software that enabled Pegasus spyware to infiltrate the devices of WhatsApp's users. This news was followed by a disclosure that the devices of certain Indians were also affected, which fact was

acknowledged by the then Hon'ble Minister of Law and Electronics and Information

Technology in a statement made in the Parliament on 20th November 2019.

5. On 15th June 2020, Citizen Lab, in collaboration with the international human rights organization, Amnesty International uncovered another spyware campaign which allegedly targeted nine individuals in India, some of whom were already suspected targets in the first spyware attack.

6. On 18th July 2021, a consortium of nearly 17 journalistic organizations from around the world, including one Indian organization, released the results of a long investigative effort indicating the alleged use of the Pegasus software on several private individuals. This investigative effort was based on a list of

some 50,000 leaked numbers which were allegedly under surveillance by clients of the NSO Group through the Pegasus software. Initially, it was discovered that nearly 300 of these

numbers belonged to Indians, many of whom are senior

journalists, doctors, political persons, and even some Court staff. At the time of filing of the Writ Petitions, nearly 10 Indians' devices were allegedly forensically analyzed to confirm the presence of the Pegasus software.

7. The above reports resulted in largescale action across the globe, with certain foreign governments even diplomatically engaging with the Israeli Government to determine the veracity of the allegations raised, while other governments have initiated proceedings internally to determine the truth of the same.

8. Respondent-Union of India, through the Hon'ble Minister of Railways, Communications and Electronics and Information Technology, took the stand in Parliament on 18th July 2021, when asked about the alleged cyberattack and spyware use, that the reports published had no factual basis. The Minister also stated that the Amnesty report itself indicated that the mere mention of a particular number in the list did not confirm whether the same was infected by Pegasus or not. Further, the Minister stated that NSO had itself factually contradicted many of the claims made in the Amnesty report. Finally, he stated that the Indian statutory and legal regime relating to surveillance and

interception of communication is extremely rigorous, and no illegal surveillance could take place.

9. Some of the Writ Petitioners before this Court allege to be direct victims of the Pegasus attack, while others are Public Interest Litigants. They raise the issue of the inaction on the part of the Respondent-Union of India to seriously consider the allegations raised, relating to the purported

cyberattack on citizens of this country. Additionally, the apprehension expressed by some Petitioners relates to the fact that, keeping in mind the NSO Group disclosure that it sold its Pegasus software only to vetted Governments, either some foreign government or certain agencies of the Respondent-Union of India are using the said software on citizens of the country without following the due procedure established under law. Therefore, to ensure credibility of the process, most of the Petitioners are seeking an

independent investigation into the allegations.

10. Before considering the issues at hand on merits, it is necessary for this Court to summarize the events that transpired in the Courtroom proceedings, to give some context to the order being passed.

11. On 10th August 2021, it was recorded by this Court that a

copy of some of the petitions in this batch had been served on the learned Solicitor General. The learned Solicitor General took an adjournment at that time to get instructions.

12. On 16th August 2021, a "limited affidavit" was placed on record by the learned Solicitor General that was filed by the Additional Secretary, Ministry of Electronics and Information Technology, Union of India. The relevant parts of the limited affidavit filed by the Respondent- Union of India are as follows:

"2. I state and submit that **due to the limited time at the disposal of the deponent/respondents, it is not possible to deal with all the facts stated and the contentions raised in the batch of petitions before this Hon'ble Court . I am therefore, filing this limited affidavit at this stage while reserving liberty to file further affidavit hereafter in detail.**

I, however, respectfully submit that my not dealing with any of the petitions para wise may not be treated as my having admitted the truthfulness or otherwise of any of the contents thereof.

3. At the outset, it is submitted that I herebyunequivocally deny any and all of the allegations made against the Respondents in the captioned petition and other connected petitions. A bare perusal of the captioned petition and other connected petitions makes it clear that the same are based on conjectures and surmises or on other unsubstantiated media reports or incomplete or uncorroborated material. It is submitted that the same cannot be the basis for invoking the writ jurisdiction of this Hon'ble Court.

4. It is submitted that this question stands already

clarified on the floor of the Parliament by the Hon'ble Minister of Railways, Communications and Electronics & Information Technology of India, Government of India. A copy of the statement of the Hon'ble Minister is attached herewith and marked as **Annexure R-1**. In that view of the matter, in the respectful submission of the deponent, nothing further needs to be done at the behest of the Petitioner, more particularly when they have not made out any case.

5. It is, however, submitted that **with a view to dispel any wrong narrative spread by certain vested interests and with an object of examining the issue raised, the Union of India will constitute a Committee of Experts in the field which will go in to all aspects of the issue**."

On that day, we heard learned senior counsel appearing on behalf of the Petitioners and the learned Solicitor General at some length and adjourned the matter for further hearing.

13. On the next date of hearing, on 17th August 2021, this Court indicated to the learned Solicitor General, while issuing notice to the Respondent-Union of India, that the limited affidavit filed by them was insufficient for the Court to come to any conclusion regarding the stand of the Respondent-Union of India with respect to the allegations raised by the Petitioners. As the limited affidavit itself recorded that the detailed facts were not adverted to due to a paucity of time, we indicated to the learned Solicitor General that we were willing to give them further time to

enable the Respondent-Union of India to file a more detailed affidavit. The learned Solicitor General indicated his

apprehension that the disclosure of certain facts might affect the national security and defense of the nation.

14. This Court clarified at that juncture that it was not interested in any information that may have a deleterious impact on the security of the country. However, the Respondent-Union of India could still place on record facts pertaining to the events highlighted by the Petitioners,

without disclosing information adjudged to be sensitive by the relevant authorities.

15. Mr. Kapil Sibal, learned senior counsel appearing for the Petitioners in Writ Petition (C) Nos. 826 and 851 of 2021, fairly stated that the Petitioners were also concerned about the national interest and would not press for any such information. The learned Solicitor General again took some time to seek instructions.

16. When the matter was next listed on 07th September 2021, the learned Solicitor General requested an adjournment, and we directed that the matter be listed on 13th September 2021.

17. On 13th September 2021, we were again informed by the learned Solicitor General that placing the information sought by

the Petitioners on an affidavit would be detrimental to the security interests of the nation. The learned Solicitor General submitted that such information could not be made a matter of public debate as the same could be used by terror groups to hamper national security. He reiterated the statement dated 18th July 2021 made by the Hon'ble Minister of Railways, Communications and Electronics and Information Technology on the floor of the Parliament regarding the statutory mechanism surrounding surveillance and interception in the country which ensures that unauthorized surveillance does not take place. He finally submitted that, to assuage the concerns of the public and to dispel any

wrong narratives, considering the technical nature of the issues, the Respondent-Union of India would be willing to constitute an Expert Committee which will go into all aspects and file a report before this Court.

18. Mr. Kapil Sibal, learned senior counsel appearing on behalf of the Petitioners in Writ Petition (C) Nos. 826 and 851 of 2021, submitted that the Respondent-Union of India should not act in a manner that would prevent the Court from rendering justice and should not withhold information from the Court in a matter concerning the alleged violation of fundamental rights of citizens.

He submitted that in the year 2019, when certain reports of Pegasus hacking WhatsApp came to light, the then Hon'ble Minister of Law and Information Technology and Communication had acknowledged the reports of hacking in Parliament, but the Respondent-Union of India had not indicated what actions were taken subsequently, which information they could have disclosed on affidavit. Learned senior counsel submitted that such inaction by the Respondent- Union was a matter of grave concern, particularly when reputed international organizations with no reason for bias against the nation had also accepted the fact of such an attack having been made. Mr. Sibal finally submitted that an independent probe into the alleged incident required to take place under the supervision of retired Judges of this Court, as was ordered by this Court in the Jain Hawala case. He objected to the suggestion of the learned

Solicitor General that the Respondent-Union of India itself be allowed to form a Committee on the ground that any Committee formed to probe the allegations raised by the Petitioners should be completely independent from the Respondent-Union of India.

19. Mr. Shyam Divan, learned senior counsel appearing on behalf of the Petitioner in Writ Petition (C) No. 849 of 2021 who

claims to be one of the parties whose phone was directly affected by Pegasus, submitted that Pegasus enabled an entity to not only surveil or spy on an individual, but also allowed them to implant false documents and evidence in a device. He relied on affidavits filed by two experts in the field of cyber security to buttress his submission regarding the nature and function of the software. Mr. Divan submitted that once such a largescale cyberattack and threat had been made public and brought to the knowledge of the Respondent-Union of India, it was the State's responsibility to take necessary action to protect the interests and fundamental rights of the citizens, particularly when there existed the risk that such an attack was made by a foreign entity. Mr. Divan pressed for the interim relief sought in Writ Petition (C) No. 849 of 2021, whereby a response was sought on affidavit from the Cabinet Secretary. Mr. Divan also supported the prayer made by Mr. Sibal regarding the constitution of a special Committee or

Special Investigation Team to probe the allegations.

20. Mr. Rakesh Dwivedi, learned senior counsel appearing on behalf of the Petitioners in Writ Petition (C) No. 853 of 2021 submitted that the Petitioners are senior journalists who are victims of the Pegasus attack. He submitted that if the

Respondent-Union of India had made a statement on affidavit that it had not used a malware or spied on the Petitioners in an unauthorized manner, that would have been the end of the matter. Instead, the Respondent-Union of India had not provided any information on affidavit. He therefore urged the Court to constitute an independent Committee under its supervision rather than allowing the Respondent-Union of India to constitute a Committee, as suggested by the learned Solicitor General, to avoid any credibility issues. He further submitted that requiring the Petitioners to hand over their phones to a Committee appointed by the Respondent-Union of India, when certain allegations had been raised against the Respondent-Union of India, would amount to a secret exercise whose results would not be trusted by the Petitioners or the public.

21. Mr. Dinesh Dwivedi, learned senior counsel appearing on behalf of the Petitioner in Writ Petition (C) No. 848 of 2021 submitted that his client is a respected journalist whose device had been infected with the Pegasus malware. The main thrust of his submission was that if any pleading was

not specifically denied, it would be deemed to have been admitted. As the Respondent-Union of India had not specifically denied the

Petitioner's allegation, the same should therefore be deemed to be admitted by the Respondent-Union of India. Learned senior counsel submitted that such an attack on the privacy of the Petitioner was not only a violation of his fundamental right, but also amounted to chilling his freedom of speech as a journalist. **22.** Ms. Meenakshi Arora, learned senior counsel appearing on behalf of the Petitioner in Writ Petition (C) No. 829 of 2021, supported the prayer made by Mr. Kapil Sibal regarding the constitution of an independent Special Investigation Team headed by a retired Judge to investigate the matter.

23. Mr. Colin Gonsalves, learned senior counsel appearing on behalf of the Petitioners in Writ Petition (C) No. 909 of 2021, wherein Petitioner No. 1 is a journalist, lawyer and human rights activist who is an affected party, while Petitioner No. 2 is a registered society which works on the promotion and protection of digital rights and digital freedom in India, submitted that a number of such digital interceptions were being conducted by the States and the Respondent-Union of India. He submitted that, in light of the allegations raised against the Respondent-Union of India in the present matter, it would not be appropriate to allow the Respondent-Union of India to form a Committee to

investigate the present allegations. Further, the learned senior counsel pointed to the actions taken by various foreign governments in light of the purported spyware attack to highlight the veracity of the reports by news agencies and the seriousness

with which the allegations were being viewed in other countries.

24. Mr. M. L. Sharma, petitioner-in-person in Writ Petition (Crl.) No. 314 of 2021, submitted that the Pegasus suite of spywares was different from other spyware as it allowed an agency to gain complete control over an individual's device. He submitted that the software could be used to plant false evidence into an individual's device, which could then be used to implicate the said person. He therefore submitted that the alleged use of

Pegasus on the citizens of the country, was of grave concern. **25.** The learned Solicitor General rebutted the arguments of the Petitioners and submitted that there was no reason to question the credibility of any Committee that might be constituted by the Respondent-Union of India as only experts independent of any association with the Respondent-Union of India would be a part of the same. He further stated that all technologies had the capability of either being used or abused, and it could not be said that the use of such a software was *per se* impermissible,

particularly when a robust legal mechanism existed to check the use of the same. He finally reiterated that this Court should allow the Respondent-Union of India to constitute an Expert Committee which would be under its supervision.

26. We have considered the submissions of the learned senior counsel for the Petitioners, Petitioner-in-person, and the learned Solicitor General for the Respondent-Union of India.

27. At the outset, certain nuances of the right to privacy in India- its facets and importance, need to be discussed. Historically, privacy rights have been 'property centric' rather than people centric. This approach was seen in both the United States of America as well as in England. In 1604, in the historical ***Semayne's*** **case, 77 ER 194 (KB)** it was famously held that "*every man's house is his castle*". This marked the beginning of the development of the law protecting people against unlawful warrants and searches.

28. As William Pitt, the Earl of Chatham stated in March 1763[1]:

> "The poorest man may in his cottage bid defiance to all the force of the Crown. It may be frail—its roof may shake—the wind may blow through it—the storm may enter, the rain may enter—but the King of England cannot enter!—all his force dares not cross the threshold of the ruined tenement!"

[1] Lord Brougham, ***Historical Sketches of Statesmen who Flourished in the Time of George III First Series***, Vol. 1 (1845).

29. As long back as in 1890, Samuel Warren and Louis Brandeis observed in their celebrated article 'The Right to Privacy'[2]:

> "Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right "to be let alone."…numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops."

30. However, unlike the 'property centric' origin of privacy rights in England and under the Fourth Amendment in the Constitution of the United States of America, in India, privacy rights may be traced to the 'right to life' enshrined under Article 21 of the Constitution. When this Court expounded on the meaning of "life" under Article 21, it did not restrict the same in a pedantic manner. An expanded meaning has been given to the right to life in India, which accepts that "life" does not refer to mere animal existence but encapsulates a certain assured quality.

31. It is in this context that we must contextualize the issues that are being raised in this batch of petitions. We live in the era of information revolution, where the entire lives of individuals are

[2] Samuel Warren and Louis Brandeis, ***The Right to Privacy***, HARVARD LAW REVIEW, Vol. 4 (5), 193 (Dec. 15, 1890).

stored in the cloud or in a digital dossier. We must recognize that while technology is a useful tool for improving the lives of the people, at the same time, it can also be used to breach that sacred private space of an individual.

32. Members of a civilized democratic society have a reasonable expectation of privacy. Privacy is not the singular concern of journalists or social activists. Every citizen of India ought to be protected against violations of privacy. It is this expectation which enables us to exercise our choices, liberties, and freedom.

This Court in ***K.S. Puttaswamy (Privacy-9J.) v. Union of India*****,**

(2017) 10 SCC 1, has recognized that the right to privacy is as sacrosanct as human existence and is inalienable to human dignity and autonomy. This Court held that:

> **"320. Privacy is a constitutionally protected right which emerges primarily from the guarantee of life and personal liberty in Article 21 of the Constitution.** Elements of privacy also arise in varying contexts from the other facets of freedom and dignity recognised and guaranteed by the fundamental rights contained in Part III.
> **…**
>
> **325.** Like other rights which form part of the fundamental freedoms protected by Part III, including the right to life and personal liberty under Article 21, privacy is not an absolute right. **A law which encroaches upon privacy will have to withstand the**

> **touchstone of permissible restrictions on fundamental rights. In the context of Article 21 an invasion of privacy must be justified on the basis of a law which stipulates a procedure which is fair,**

just and reasonable. The law must also be valid with reference to the encroachment on life and personal liberty under Article 21. An invasion of life or personal liberty must meet the threefold requirement of (*i*) legality, which postulates the existence of law; (*ii*) need, defined in terms of a legitimate State aim; and (*iii*) proportionality which ensures a rational nexus between the objects and the means adopted to achieve them."

(*emphasis supplied*)

33. Although declared to be inalienable, the right to privacy of course cannot be said to be an absolute, as the Indian Constitution does not provide for such a right without reasonable restrictions. As with all the other fundamental rights, this Court therefore must recognize that certain limitations exist when it comes to the right to privacy as well. However, any restrictions imposed must necessarily pass constitutional scrutiny. **34.** In ***K.S. Puttaswamy (Privacy-9J.)*** **(*supra*),** this Court considered the need to protect the privacy interests of individuals while furthering legitimate State interests. This Court therefore directed the State to embark upon the exercise of balancing of competing interests. This Court observed as follows:

"310.While it intervenes to protect legitimate

State interests, the State must nevertheless put into place a robust regime that ensures the fulfilment of a threefold requirement. These three requirements apply to all restraints on privacy (not just informational privacy). They emanate from the procedural and content-based mandate of Article

21. The first requirement that there must be a law in existence to justify an encroachment on privacy is an express requirement of Article 21. For, no person can be deprived of his life or personal liberty except in accordance with the procedure established by law.

> The existence of law is an essential requirement. Second, the requirement of a need, in terms of a legitimate State aim, ensures that the nature and content of the law which imposes the restriction falls within the zone of reasonableness mandated by Article 14, which is a guarantee against arbitrary State action. The pursuit of a legitimate State aim ensures that the law does not suffer from manifest arbitrariness. Legitimacy, as a postulate, involves a value judgment. Judicial review does not reappreciate or second guess the value judgment of the legislature but is for deciding whether the aim which is sought to be pursued suffers from palpable or manifest arbitrariness. **The third requirement ensures that the means which are adopted by the legislature are proportional to the object and needs sought to be fulfilled by the law. Proportionality is an essential facet of the guarantee against arbitrary State action because it ensures that the nature and quality of the encroachment on the right is not disproportionate to the purpose of the law. Hence, the threefold requirement for a valid law arises out of the mutual interdependence between the fundamental guarantees against arbitrariness on the one hand and the protection of life and personal liberty, on the other. The right to privacy, which is an intrinsic part of the right to life and liberty, and the freedoms embodied in Part III is subject to the**

> **same restraints which apply to those freedoms."**

(*emphasis supplied*) 35. The right to privacy is directly infringed when there is surveillance or spying done on an individual, either by the State or by any external agency. Ellen Alderman and Caroline Kennedy, in 'Right to Privacy',[3] foresaw this threat to privacy in 1995, while referring to governmental eavesdropping in the United States of America, in the following words:

> "Perhaps the scariest threat to privacy comes in the area known as "informational privacy". Information about all of us is now collected not only by the old standbys, the IRS and FBI, but also by

[3] Ellen Alderman and Caroline Kennedy, THE RIGHT TO PRIVACY, 223 (1995).

> the MTB, MIB, NCOA, and NCIC, as well as credit bureaus, credit unions, and credit card companies. We now have cellular phones, which are different from cordless phones, which are different from what we used to think of as phones. We worry about e-mail, voice mail, and junk mail. And something with the perky name Clipper Chip - developed specifically to allow governmental eavesdropping on coded electronic communications – is apparently the biggest threat of all."

36. Of course, if done by the State, the same must be justified on constitutional grounds. This Court is cognizant of the State's interest to ensure that life and liberty is preserved and must balance the same. For instance, in today's world, information gathered by intelligence agencies through surveillance is essential for the fight against violence and terror. To access this

information, a need may arise to interfere with the right to privacy of an individual, provided it is carried out only when it is absolutely necessary for protecting national security/interest and is proportional. The considerations for usage of such alleged technology, ought to be evidence based. In a democratic country governed by the rule of law, indiscriminate spying on individuals cannot be allowed except with sufficient statutory safeguards, by following the procedure established by law under the

Constitution.

37. This trade-off between the right to privacy of an individual and the security interests of the State, has been recognized world over with the renowned scholar ***Daniel Solove***[4] commenting on the same as follows:

> "The debate between privacy and security has been framed incorrectly, with the trade-off between these values understood as an all-or-nothing proposition. **But protecting privacy need not be fatal to security measures; it merely demands oversight and regulation. We can't progress in the debate between privacy and security because the debate itself is flawed**.
>
> The law suffers from related problems. It seeks to balance privacy and security, but systematic problems plague the way the balancing takes place….

> Privacy often can be protected without undue cost to security. In instances when adequate compromises can't be achieved, the trade-off can be made in a manner that is fair to both sides. We can reach a better balance between privacy and security. We must. There is too much at stake to fail."

(*emphasis supplied*) 38. Somewhat allied to the concerns of privacy, is the freedom of the press. Certain observations made by this Court in the case of ***Indian Express Newspapers (Bombay) Private Limited v. Union of India,*** **(1985) 1 SCC 641** may be extracted:

> **"25.** The freedom of press, as one of the members of the Constituent Assembly said, is one of the items around which the greatest and the bitterest of constitutional struggles have been

[4] Daniel J. Solove, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY (2011).

> waged in all countries where liberal constitutions prevail. The said freedom is attained at considerable sacrifice and suffering and ultimately it has come to be incorporated in the various written constitutions…"

39. It is undeniable that surveillance and the knowledge that one is under the threat of being spied on can affect the way an individual decides to exercise his or her rights. Such a scenario might result in self-censorship. This is of particular concern when it relates to the freedom of the press, which is an important pillar of democracy. Such chilling effect on the freedom of speech is an assault on the vital public-watchdog role of the press, which may undermine the ability of the press to provide accurate

and reliable information. Recently, in the case of ***Anuradha Bhasin v. Union of India*****, (2020) 3 SCC 637,** this Court highlighted the importance of freedom of the press in a modern democracy in the following words:

> **"159.** In this context, one possible test of chilling effect is comparative harm. **In this framework, the Court is required to see whether the impugned restrictions, due to their broad-based nature, have had a restrictive effect on similarly placed individuals during the period.** It is the contention of the petitioner that she was not able to publish her newspaper from 6-8-2019 to 11-10-2019. However, no evidence was put forth to establish that such other individuals were also restricted in publishing newspapers in the area. Without such evidence having been placed on record, it would be impossible to distinguish a legitimate claim of chilling effect from a mere emotive argument for a self-serving purpose. On the other hand, the learned Solicitor General has submitted that there were other newspapers which were running

> during the aforesaid time period. In view of these facts, and considering that the aforesaid petitioner has now resumed publication, we do not deem it fit to indulge more in the issue than to state that responsible Governments are required to respect the freedom of the press at all times. **Journalists are to be accommodated in reporting and there is no justification for allowing a sword of Damocles to hang over the press indefinitely**."

(*emphasis supplied*) 40. An important and necessary corollary of such a right is to ensure the protection of sources of information. Protection of journalistic sources is one of the basic conditions for the freedom

of the press. Without such protection, sources may be deterred from assisting the press in informing the public on matters of public interest.

41. Having regard to the importance of the protection of journalistic sources for press freedom in a democratic society and the potential chilling effect that snooping techniques may have, this Court's task in the present matter, where certain grave allegations of infringement of the rights of the citizens of the country have been raised, assumes great significance. In this light, this Court is compelled to take up the cause to determine the truth and get to the bottom of the allegations made herein. **42.** Initially, this Court was not satisfied with the Writ Petitions that were filed as the same were completely reliant only upon certain newspaper reports. This Court has generally attempted to discourage Writ Petitions, particularly Public Interest Litigations, which are based entirely on newspaper reports without any additional steps taken by the Petitioner. In

this respect, it may be relevant to quote the observations of this Court in the case of

***Rohit Pandey v. Union of India*, (2005) 13 SCC 702,** which are as follows:

"**1.** …The **only basis for the petitioner coming to**

this Court are two newspaper reports dated 25-1-2004, and the other dated 12-2-2004. This petition was immediately filed on 16-2-2004 after the aforesaid second newspaper report appeared….

2. We expect that when such a petition is filed in public interest and particularly by a member of the legal profession, it would be filed with all seriousness and after doing the necessary homework and enquiry. If the petitioner is so publicspirited at such a young age as is so professed, the least one would expect is that an enquiry would be made from the authorities concerned as to the nature of investigation which may be going on before filing a petition that the investigation be conducted by the Central Bureau of Investigation. Admittedly, no such measures were taken by the petitioner. There is nothing in the petition as to what, in fact, prompted the petitioner to approach this Court within two-three days of the second publication dated 12-2-2004, in the newspaper Amar Ujala. Further, the State of Uttar Pradesh had filed its affidavit a year earlier i.e. on 710-2004, placing on record the steps taken against the accused persons, including the submission of the charge-sheet before the appropriate court. Despite one year having elapsed after the filing of the affidavit by the Special Secretary to the Home Department of the Government of Uttar Pradesh, nothing seems to have been done by the petitioner. The petitioner has not even controverted what is stated in the affidavit. Ordinarily, we would have dismissed such a misconceived petition with exemplary costs but considering that the petitioner is a young advocate, we feel that the ends of justice would be met and the necessary message conveyed if a token cost of rupees one thousand is imposed on the petitioner."

(*emphasis supplied*) 43. While we understand that the allegations made in these petitions pertain to matters about which ordinary citizens would

not have information except for the investigating reporting done by news agencies, looking to the quality of some of the petitions filed, we are constrained to observe that individuals should not file half-baked petitions merely on a few newspaper reports. Such an exercise, far from helping the cause espoused by the individual filing the petition, is often detrimental to the cause itself. This is because the Court will not have proper assistance in the matter, with the burden to even determine preliminary facts being left to the Court. It is for this reason that trigger happy filing of such petitions in Courts, and more particularly in this Court which is to be the final adjudicatory body in the country, needs to be discouraged. This should not be taken to mean that the news agencies are not trusted by the Court, but to emphasize the role that each pillar of democracy occupies in the polity. News agencies report facts and bring to light issues which might otherwise not be publicly known. These may then become the basis for further action taken by an active and concerned civil society, as well as for any subsequent filings made in Courts. But newspaper reports, in and of themselves, should not in the ordinary course be taken to be ready-made pleadings that may be filed in Court.

44. That said, after we indicated our reservations to the Petitioners regarding the lack of material, various other petitions have been filed in Court, including by individuals who were purportedly victims of the alleged Pegasus spyware attack. These subsequently filed petitions, as well as additional documents filed by others, have brought on record certain materials that cannot be brushed aside, such as the reports of reputed organizations like Citizen Lab and affidavits of experts. Additionally, the sheer volume of cross-referenced and crossverified reports from various reputable news organizations across the world along with the reactions of foreign governments and legal institutions also moved us to consider that this is a case where the jurisdiction of the Court may be exercised. Of course, the learned Solicitor General suggested that many of these reports are motivated and self-serving. However, such an omnibus oral allegation is not sufficient to desist from

interference.

45. It is for this reason that this Court issued notice to the Respondent-Union of India and sought information from them. We would like to re-emphasize what is already apparent from the record of proceedings. This Court gave ample opportunity to the

Respondent-Union of India to clarify its stand regarding the allegations raised, and to provide information to assist the Court regarding the various actions

taken by it over the past two years, since the first disclosed alleged Pegasus spyware attack. We had made it clear to the learned Solicitor General on many occasions that we would not push the Respondent-Union of India to provide any information that may affect the national security concerns of the country. However, despite the repeated assurances and opportunities given, ultimately the Respondent-Union of India has placed on record what they call a "limited affidavit", which does not shed any light on their stand or provide any clarity as to the facts of the matter at hand. If the Respondent-Union of India had made their stand clear it would have been a different situation, and the burden on us would have been different.

46. Such a course of action taken by the Respondent-Union of India, especially in proceedings of the present nature which touches upon the fundamental rights of the citizens of the country, cannot be accepted. As held by this Court in ***Ram Jethmalani v. Union of India,*** **(2011) 8 SCC 1**, the Respondent-Union of India should not take an adversarial position when the fundamental rights of citizens are at threat.

This Court in that case observed as follows:

> **"75.** In order that the right guaranteed by clause (1) of Article 32 be meaningful, and particularly because such petitions seek the protection of fundamental rights, it is imperative that in such proceedings the petitioners are not denied the information necessary for them to properly articulate the case and be heard,

especially where such information is in the possession of the State. To deny access to such information, without citing any constitutional principle or enumerated grounds of constitutional prohibition, would be to thwart the right granted by clause (1) of Article 32.

76. Further, inasmuch as, by history and tradition of common law, judicial proceedings are substantively, though not necessarily fully, adversarial, **both parties bear the responsibility of placing all the relevant information, analyses, and facts before this Court as completely as possible. In most situations, it is the State which may have more comprehensive information** that is relevant to the matters at hand in such proceedings...

77. It is necessary for us to note that the burden of asserting, and proving, by relevant evidence a claim in judicial proceedings would ordinarily be placed upon the proponent of such a claim; however, **the burden of protection of fundamental rights is primarily the duty of the State. Consequently, unless constitutional grounds exist, the State may not act in a manner that hinders this Court from rendering complete justice in such proceedings**. Withholding of information from the petitioners, or seeking to cast the relevant events and facts in a light favourable to the State in the context of the proceedings, even though ultimately detrimental to the essential task of protecting fundamental rights, would be destructive to the

guarantee in clause (1) of Article 32…

78. In the task of upholding of fundamentalrights, the State cannot be an adversary. The State has the duty, generally, to reveal all the facts and information in its possession to the Court, and also provide the same to the petitioners. This is so, because the petitioners would also then be enabled to bring to light facts and the law that may be relevant for the Court in rendering its decision. In proceedings such as those under Article 32, both the petitioner and the State, have to necessarily be the eyes and ears of the Court. Blinding the petitioner would substantially detract from the integrity of the process of judicial

decisionmaking in Article 32 proceedings, especially where the issue is of upholding of fundamental rights.**"**

(*emphasis supplied*)

47. This free flow of information from the Petitioners and the State, in a writ proceeding before the Court, is an important step towards Governmental transparency and openness, which are celebrated values under our Constitution, as recognized by this

Court recently in the ***Anuradha Bhasin* (*supra*)** judgment**.**

48. Of course, there may be circumstances where the State has a constitutionally defensible reason for denying access to certain information or divulging certain information as was recognized by this Court in the ***Ram Jethmalani* (*supra*)** case, as extracted below:

"80. <u>Withholding of information from the</u>

<u>petitioners by the State</u>, thereby constraining their freedom of speech and expression before this Court, **<u>may be premised only on the exceptions carved out, in clause (2) of Article 19, "in 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 by law that demarcate exceptions, provided that such a law comports with the enumerated grounds in clause</u>**

<u>(2) of Article 19</u>, or that may be provided for elsewhere in the Constitution."

(*emphasis supplied*)

49. It is on the strength of the above exception carved out that the Respondent-Union of India has justified its non-submission of a detailed counter

affidavit, *viz.*, by citing security concerns. It is a settled position of law that in matters pertaining to national security, the scope of judicial review is limited. However, this does not mean that the State gets a free pass every time the spectre of "national security" is raised. National security cannot be the bugbear that the judiciary shies away from, by virtue of its mere mentioning. Although this Court should be circumspect in encroaching upon the domain of national security, no omnibus prohibition can be called for against judicial review.

50. Of course, the Respondent-Union of India may decline to provide information when constitutional considerations exist,

such as those pertaining to the security of the State, or when there is a specific immunity under a specific statute. However, it is incumbent on the State to not only specifically plead such constitutional concern or statutory immunity but they must also prove and justify the same in Court on affidavit. The RespondentUnion of India must necessarily plead and prove the facts which indicate that the information sought must be kept secret as their divulgence would affect national security concerns. They must justify the stand that they take before a Court. The mere invocation of national security by the State does not render the

Court a mute spectator.

51. In the present matter, as we have indicated above, the Petitioners have placed on record certain material that *prima facie* merits consideration by this

Court. There has been no specific denial of any of the facts averred by the Petitioners by the Respondent-Union of India. There has only been an omnibus and vague denial in the "limited affidavit" filed by the Respondent-Union of India, which cannot be sufficient. In such circumstances, we have no option but to accept the *prima facie* case made out by the Petitioners to examine the allegations made.

34

52. Different forms of surveillance and data gathering by intelligence agencies to fight terrorism, crime and corruption in national interest and/or for national security, are accepted norms all over the world. The Petitioners do not contend that the State should not resort to surveillance/collection of data in matters of national security. The complaint of the Petitioners is about the misuse or likely misuse of spyware in violation of the right to privacy of citizens. The Respondent-Union of India also does not contend that its agencies can resort to surveillance/collection of data relating to its citizens where national security and national interest are not involved. The apprehension of the Respondent-Union of India is that any inquiry in this behalf should not jeopardize national security and the steps taken by it to protect national security. There is thus a broad consensus that unauthorized surveillance/accessing of stored data from the phones and other devices of citizens for reasons other than nation's security would be illegal, objectionable and a matter of concern.

53. The only question that remains then is what the appropriate remedy in this case would be. Mr. Shyam Divan, learned senior counsel appearing on behalf of the Petitioner in Writ Petition (C)

No. 849 of 2021 sought an interim order from this Court directing the Cabinet Secretary to put certain facts on an affidavit. On the other hand, most of the other senior counsel appearing on behalf of the other Writ Petitioners sought an independent investigation or inquiry into the allegations pertaining to the use of Pegasus software either by constituting a Special Investigation Team headed by a retired judge or by a

Judges' Committee.

54. We are of the opinion that in the circumstances of the present case, when the Respondent-Union of India has already been given multiple opportunities to file an affidavit on record, and looking to the conduct of the Respondent-Union of India in not placing on record any facts through their reliance on the "national security" defense, no useful purpose would be served by issuing directions of the nature sought by Mr. Shyam Divan, apart from causing a further delay in proceedings.

55. Instead, we are inclined to pass an order appointing an Expert Committee whose functioning will be overseen by a retired Judge of the Supreme Court. Such a course of action has been adopted by this Court in various other

circumstances when the Court found it fit in the facts and circumstances of the case to

probe the truth or falsity of certain allegations, taking into account the public importance and the alleged scope and nature of the large-scale violation of the fundamental rights of the citizens of the country [***See Ram Jethmalani* (*supra*); *ExtraJudicial Execution Victim Families Association v. Union of India*, (2013) 2 SCC 493; *G.S. Mani v. Union of India,* order dated 12.12.2019 in W.P. (Crl.) No. 348 of 2019].**

56. The compelling circumstances that have weighed with us to pass such an order are as follows:

i. Right to privacy and freedom of speech are alleged to be impacted, which needs to be examined.

ii. The entire citizenry is affected by such allegations due to the potential chilling effect.

iii. No clear stand taken by the Respondent-Union of India regarding actions taken by it.

iv. Seriousness accorded to the allegations by foreign countries and involvement of foreign parties.

v. Possibility that some foreign authority, agency or private entity is involved in placing citizens of this country under surveillance.

vi. Allegations that the Union or State Governments are party

to the rights' deprivations of the citizens.

vii. Limitation under writ jurisdiction to delve into factual aspects. For instance, even the question of usage of the technology on citizens, which is the jurisdictional fact, is disputed and requires further factual examination.

57. It is for reason **(vi)** above that we decline the RespondentUnion of India's plea to allow them to appoint an Expert Committee for the purposes of investigating the allegations, as such a course of action would violate the settled judicial principle against bias, *i.e.*, that '*justice must not only be done, but also be seen to be done*'.

58. At this juncture, it would be appropriate to state that in this world of conflicts, it was an extremely uphill task to find and select experts who are free from prejudices, are independent and competent. Rather than relying upon any Government agencies or any, we have constituted the Committee and shortlisted expert members based on biodatas and information collected independently. Some of the candidates politely declined this assignment, while others had some conflict of interest. With our best intentions and efforts, we have shortlisted and chosen the most renowned experts available to be a part of the Committee.

Additionally, we have also left it to the discretion of the learned overseeing judge to take assistance from any expert, if necessary, to ensure absolute transparency and efficiency, as directed in paragraph 62(3).

59. With the above observations, we constitute a Technical Committee comprising of three members, including those who are experts in cyber security, digital forensics, networks and hardware, whose functioning will be overseen by Justice R.V. Raveendran, former Judge, Supreme Court of India. The learned overseeing Judge will be assisted in this task by:

i. Mr. Alok Joshi, former IPS officer (1976 batch) who has immense and diverse investigative experience and technical knowledge. He has worked as the Joint Director, Intelligence Bureau, the Secretary(R), Research and Analysis Wing and Chairman, National Technical Research Organisation. **ii.** Dr. Sundeep Oberoi, Chairman, ISO/IEC JTC1 SC7 (International Organisation of Standardisation/ International Electro-Technical Commission/Joint Technical Committee), a sub-committee which develops and facilitates standards within the field of

software products and systems. Dr. Oberoi is also a part of the Advisory Board of Cyber Security Education and Research Centre at

Indraprastha Institute of Information Technology, Delhi. He is globally

recognized as a cyber security expert.

60. The three members Technical Committee [*hereinafter referred to as the* ***"Committee"***] shall comprise of:

i. Dr. Naveen Kumar Chaudhary, Professor (Cyber Security and Digital Forensics) and Dean, National Forensic Sciences University, Gandhinagar, Gujarat. Dr. Chaudhary has over two decades of experience as an academician, cyber security enabler and cyber security expert. He specializes in cyber security policy, network vulnerability assessment and penetration

testing.

ii. Dr. Prabaharan P., Professor (School of Engineering), Amrita Vishwa Vidyapeetham, Amritapuri, Kerala. He has two decades of experience in computer science and security areas. His areas of interest are malware detection, critical infrastructural security, complex binary analysis, AI and machine learning. He has

many publications in reputed journals.

iii. Dr. Ashwin Anil Gumaste, Institute Chair Associate Professor (Computer Science and Engineering), Indian Institute of Technology, Bombay, Maharashtra. He has been granted 20 US

patents and has published over 150 papers and authored 3 books in his field. He has received several National awards including the Vikram Sarabhai Research Award (2012) and Shanti Swarup Bhatnagar Prize for Science and Technology (2018). He has also held the position of Visiting Scientist at the Massachusetts Institute of Technology, USA.

61. The terms of reference of the Committee are as follows:

A. To enquire, investigate and determine:

i. 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 not explicitly stated herein?

ii. The details of the victims and/or persons affected by such a spyware attack.

iii. What steps/actions have been taken by the Respondent-Union of India after reports were published in the year 2019 about hacking of WhatsApp accounts of Indian citizens, using the Pegasus suite of spyware. iv. Whether any Pegasus suite of spyware was acquired by

the Respondent-Union of India, or any State Government, or any central or state agency for use against the citizens of India?

v. If any governmental agency has used the Pegasus suite of spyware on the citizens of this country, under what law, rule, guideline, protocol or lawful procedure was such deployment made?

vi. If any domestic entity/person has used the spyware on the citizens of this country, then is such a use authorised?

vii. Any other matter or aspect which may be connected, ancillary or incidental to the above terms of reference, which the Committee may deem fit and proper to

investigate.

B. To make recommendations:

i. Regarding enactment or amendment to existing law and procedures surrounding surveillance and for

securing improved right to privacy.

ii. Regarding enhancing and improving the cyber security of the nation and its assets.

iii. To ensure prevention of invasion of citizens' right to privacy, otherwise than in accordance with law, by State and/or non-State entities through such spywares.

iv. Regarding the establishment of a mechanism for

citizens to raise grievances on suspicion of illegal surveillance of their devices.

v. Regarding the setting up of a well-equipped independent premier agency to investigate cyber security vulnerabilities, for threat assessment relating to cyberattacks and to investigate instances of cyberattacks in the country.

vi. Regarding any *ad-hoc* arrangement that may be made by this Court as an interim measure for the protection of citizen's rights, pending filling up of lacunae by the

Parliament.

vii. On any other ancillary matter that the Committee may deem fit and proper.

62. The Procedure of the Committee shall be as follows:

(1) The Committee constituted by this Order is authorised to (a) devise its own procedure to effectively implement and

answer the Terms of Reference;

(b) hold such enquiry or investigation as it deems fit;and (c) take statements of any person in connection with the enquiry and call for the records of any authority or individual.

(2) Justice R. V. Raveendran, former Judge, Supreme Court ofIndia will oversee the functioning of the Committee with respect to the

methodology to be adopted, procedure to be followed, enquiry and investigation that is carried out and preparation of the report.

(3) The learned overseeing Judge is at liberty to take the assistance of any serving or retired officer(s), legal expert(s) or technical expert(s) in discharge of his functions.

(4) We request the learned overseeing Judge to fix the honorarium of the members of the Committee in consultation with them, which shall be paid by the Respondent-Union of India immediately.

(5) The Respondent-Union of India and all the State Governments, as well as agencies/authorities under them, are directed to extend full facilities, including providing support with respect to infrastructure needs, manpower, finances, or any other matter as may be required by the Committee or the overseeing former Judge to effectively and expeditiously carry out the task assigned to them by this Court.

(6) Mr. Virender Kumar Bansal, Officer on Special Duty/ Registrar, Supreme Court of India, is directed to coordinate between the Committee, the learned overseeing Judge and the Central/State Governments to facilitate communication and ensure smooth functioning and expeditious response to, and implementation of, requests made by the Committee, the learned

overseeing Judge or those named in paragraph 59 above, tasked to assist him.

63. The Committee is requested to prepare the report after a thorough inquiry and place it before this Court, expeditiously.

64. List the matter after 8 weeks.

.....CJI. (N.V. RAMANA)

.....J.
(SURYA KANT)

.....J.
(HIMA KOHLI)

NEW DELHI;
OCTOBER 27, 2021