IN THE SUPREME COURT OF INDIA
CIVIL ORIGINAL JURISDICTION

WRIT PETITION (CIVIL) NO. OF 2021
(Under Article 32 of the Constitution of India)

(Public Interest Litigation)

IN THE MATTER OF:-

The Editors Guild of India & Anr. … Petitioners

VERSUS

Union of India & Ors. … Respondents

WITH

I.A. NO. _____ OF 2021: Application for exemption from filing notarized affidavits

PAPER – BOOK

[FOR INDEX KINDLY SEE INSIDE]

AOR FOR THE PETITIONERS: LZAFEER AHMAD B F
(Code:2941)

A4

RECORD OF PROCEEDINGS

Sl No.	DATE OF RECORD OF PROCEEDINGS	PAGES
1.		—
2.		—
3.		—
4.		—
5.		—
6.		—
7.		—
8.		—
9.		—

SYNOPSIS

The Petitioner is a registered society founded in 1978 with the twin objectives of protecting press freedom and for raising the standards of editorial leadership of newspapers and magazines. Over the last four decades, the Petitioner society has resisted infringements on the ability of journalists to engage in the free flow of ideas, and to raise accountability for public actors through public deliberation. The present public interest petition seeks enforcement of the freedom of the press from interference through spying, hacking, and electronic surveillance. The petition also seeks to enforce the *right to know* on behalf of all citizens of India about the violation of fundamental rights, abuse of power, and commission of criminal offences through use of electronic surveillance, hacking and spyware against Indian citizens. The petition further seeks a fair and impartial investigation by a special investigation team appointed by and under continued monitoring by this Hon'ble Court. Finally, the petition seeks a complete overhaul of the architecture for surveillance by challenging the constitutional vires of Section 5 of the Indian Telegraph Act, 1885, Rule 419A of the Indian Telegraph Rules 1951, Section 69 of the Information Technology Act, 2000 and Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption) of Information Rules, 2009.

On 18.07.2021, a consortium of 17 journalistic organisations of long-standing repute across the globe released the results of a months long investigative report on the use of 'Pegasus', a military grade spyware created by the Israeli cyber-arms 'NSO Group,' against journalists, political leaders, persons holding high

constitutional office, doctors, heads of intelligence, public officials, survivors of sexual harassment, lawyers, human rights defenders, and ordinary citizens in several countries including India. The investigation and reporting are led by Paris based non-profit media organisation 'Forbidden Stories', and, Amnesty International, a Nobel Peace Prize winning international human rights organisation headquartered in London. Over 80 journalists from 40 countries participated in the consortium's investigations.

The 'NSO Group' has categorically maintained that it only sells and licenses its products to "vetted governments." It's product, Pegasus, is a 'malware' that infects electronic devices and spies on the victim by transferring data to a master server in an unauthorised manner. The investigations uncovered that Pegasus was detected to have been used on several smart phones that were forensically examined by experts. Amongst 37 forensically verified cases, Pegasus was detected on the phones of 10 Indians. Forensic examination by cyber experts have confirmed the use of Pegasus infection in the phones of the following senior journalists: (i) S.N.M Abidi (Senior Journalist), (ii) Sushant Singh (Previously at Indian Express), (iii) M.K. Venu (Founder, The Wire), (iv) Siddharth Varadarajan (Founder, The Wire), and (v) Paranjoy Guha Thakurta (Senior Journalist). Attempts at hacking was detected on the phones of: (i) Vijaita Singh (Senior Journalist at The Hindu), (ii) Smita Sharma (Previously with TV18).

The report alleges that forensic analysis detected that Pegasus was installed on phones, *inter alia*, through a "zero-click process": it does not require any action by the targeted phone's user, and can remotely infiltrate a device. Pegasus is capable of

astronomical surveillance which includes accessing every bit of stored data on one's phone; real time access to emails, texts, phone calls; controlling all cameras on the device; activating the sound recording function; transmitting all sounds in the vicinity of the device; detecting whether two phones have come in physical proximity; activating features even when the phone is switched off, and more.

The consortium also investigated a leaked list of over 50,000 numbers, which were allegedly selected for surveillance by clients of the NSO Group. The reports state that the *"list does not identify who put the numbers on it, or why, and it is unknown how many of the phones were targeted or surveilled. But forensic analysis of the 37 smartphones shows that many display a tight correlation between time stamps associated with a number on the list and the initiation of surveillance, in some cases as brief as a few seconds."* Among 1500 verified numbers from this list, around 300 are Indian numbers of Indian citizens. This allegedly includes over 40 journalists, major opposition figures, one constitutional authority, two serving ministers in the Government of India, current and former heads of intelligence, and business persons.

Most alarmingly, the list allegedly includes former Election Commissioner, Shri Ashok Lavasa; Shri Rahul Gandhi of the Indian National Congress; Shri Abhishek Bannerjee of the Trinamool Congress Party; Shri Prashant Kishor (political strategist); Shri G. Parameshwara (Deputy chief minister in the JD(S)-Congress coalition government in Karnataka, which was toppled after several MLAs defected to the Bharatiya Janata Party); Shri Satish (Personal secretary to Shri H.D. Kumaraswamy, who

was chief minister of Karnataka); and Shri Venkatesh (Personal secretary to Shri Siddaramaiah, who was the Congress chief minister of Karnataka before Shri H. D Kumaraswamy).

In the face of NSO Group's stated position that it only sells to "vetted governments," these allegations of spying raise grave concerns of abuse of office; dismantling of separation of power; infringement of fundamental rights to privacy, freedom of speech and expression, and freedom of the press; subversion of the democratic process; and commission of serious criminal offences. The Pegasus cyber-attacks, *prima facie*, disclose the commission of several serious offences under the Information Technology Act, 2000; the Indian Penal Code, 1860; the Indian Telegraph Act, 1885; and the Official Secrets Act, 1923.

Journalists are tasked with enforcing the public's right to be informed, to accountability, and to open and transparent government. The Petitioner's members and all journalists have the duty in our democracy of holding all branches of government accountable by seeking information, explanations and constitutionally valid justifications for state action and inaction. To be able to fulfil this role, freedom of the press must be safeguarded. Freedom of the press relies on non-interference by the government and its agencies in reporting of journalists, including their ability to securely and confidentially speaking with sources, investigate abuse of power and corruption, expose governmental incompetence, and speak with those in opposition to the government.

The citizens of India have a right to know if the Executive government is infringing the limits of their authority under the

Constitution and what steps have been taken to safeguard their fundamental rights. The Petitioners are before this Hon'ble Court to seek the enforcement of this right, in performance of their obligations as trustees of the public, and on behalf of all citizens of India. It is regretfully submitted that all attempts to seek accountability and enforce constitutional limits through Parliamentary processes have been stonewalled. Through their intransigence, the Respondents have deliberately avoided public debate on this issue and have provided obfuscated answers, forcing the Petitioner to approach this Hon'ble Court.

The Petitioners also seek a court appointed Special Investigation Team monitored by this Hon'ble Court to investigate every aspect of the use of Pegasus by the Government of India and against Indian citizens, especially journalists. Finally, the Petitioner have challenged the constitutional vires of electronic surveillance, hacking and use of spyware, and the existing legal architecture for surveillance, in light of the gigantic leaps in technology and surveillance capabilities. The indiscriminate use of these capabilities against journalists and other democratic actors destroys freedom of speech and poisons the heart of democratic accountability. The Petitioners, are therefore, constrained to seek the intervention of this Hon'ble Court in enforcing Rule of Law, public accountability, ensuring law and order, and safeguarding of fundamental rights, including freedom of speech and expression, freedom of the press, and privacy.

Hence the present petition.

LIST OF DATES

Date	Event
18.12.1996	This Hon'ble Court delivered judgement in the case of ***PUCL v. Union of India***, reported in (1997) 1 SCC 301, on interception of telecommunications under the Indian Telegraph Act, 1885. This Hon'ble Court held that the right to privacy is a part of the right to life and personal liberty under Article 21 of the Constitution of India. Any procedure under law authorising phone tapping must be just, fair and reasonable and not unreasonably infringe upon the right to privacy.
17.10.2000	The onset of the internet revolution brought unique innovations and challenges for all spheres of human civilisation, including law and order. To meet these new challenges, and pursuant to the adoption of the Model Law on Electronic Commerce by the United Nations Commission on International Trade Law, vide General Assembly of the United Nations Resolution A/RES/51/162, the Information Technology Act, 2000 was passed by the Indian Parliament (the IT Act, 2000). The IT Act, 2000 comprehensively regulates all nature of activities and communications on electronic communication devices. This includes • prohibiting accessing, copying, extracting, contaminating, damaging, disrupting, altering, stealing from, and blocking access to any computer,

	computer system or computer network, without permission from the owner/person in charge [Section 43 and 66]. • prohibiting fraudulent or dishonest use of passwords [Section 66C]; • prohibiting capture/publishing/transmitting images of private areas of a person without her consent [Section 66E]; • prohibiting cyber-terrorism [Section 66F]; • prohibiting breach of confidentiality and privacy [Section 72]. Section 69 of the IT Act, 2000 authorised the 'Controller' appointed under the Act to, by order, direct any agency of the Government to intercept any information transmitted through any computer resource, if she is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing.
01.03.2007	The Indian Telegraph (Amendment) Rules, 2007 were notified. These rules inserted Rules 419A into the Indian Telegraph Rules, 1951, which instituted a procedure for interception of telecommunications. Rule 419A comprises a modified version of the ***PUCL v. Union of India (supra)*** guidelines with allowances for *post facto* interception orders for "operational reasons" or in "remote locations",

	amongst other flexibilities.
27.10.2009	The Information Technology (Amendment) Act, 2008 (Act No. 10 of 2009) was brought into force. This substituted the erstwhile Section 69 of the IT Act, 2000 with a completely new provision that empowered the Central and State governments to authorise interception, monitoring or decryption of information on a computer resource. The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption) of Information Rules, 2009 (the Interception Rules, 2009) also came into force and provided the procedure for the same.
24.08.2017	A nine-judge bench of this Hon'ble Court unanimously affirmed that the right to privacy is a fundamental right guaranteed by the Constitution of India in the case of ***K.S. Puttaswamy v Union of India*** reported in (2017) 10 SCC 1 thereby guaranteeing to citizens the right to live life with privacy and personal dignity. Privacy was held to include informational privacy.
18.09.2018	Citizen Lab, an interdisciplinary laboratory based at the prestigious Munk School of Global Affairs and Public Policy, University of Toronto, Canada, published a research report to the effect that an Israeli cyber-warfare vendor "NSO Group" had produced and is selling a mobile spyware suite named 'Pegasus' for invasive (including

	trans-border) surveillance against individuals. Citizen Lab found suspected Pegasus infections in 45 countries including India. **Pegasus** is beyond any simple interception tool, and is capable of a range of spyware operations from accessing every bit of stored data on one's phone to real time access to emails, texts, phone calls, to controlling all cameras on the device, to activating the sound recording function, to transmitting all sounds in the vicinity of the device, to detecting whether two phones have come in physical proximity. The NSO Group states on its website that its products are "**used exclusively by government intelligence and law enforcement agencies**.'
20.12.2018	Notification bearing S.O. 6227(E), the Union of India authorised 10 of its agencies under Rule 4 of the IT Interception Rules, 2009 for the purposes of interception, monitoring and decryption of any information generated, transmitted, received or stored in any computer resource as contemplated by Section 69 of the IT Act, 2000
January, 2019	Following the decision in ***Puttaswamy (supra)***, the constitutional vires of Section 69 of the IT Act, 2000; the IT Interception Rules, 2009, and the Notification S.O. 6227(E) dated 20.12.2018 were challenged before this Hon'ble Court in Writ Petition (Civil) No. 44 of 2019

	(tagged with others) in which this Hon'ble Court was pleased to issue notice on 14.01.2019. These provisions, along with Rule 419A of the Indian Telegraph Rules, 1951 were also challenged in Writ Petition (Civil) No. 61 of 2019 in which this Hon'ble Court was pleased to issue notice on 25.01.2019
May, 2019	WhatsApp Inc. identified a vulnerability in its phone application which allowed attackers to inject spyware in the targets software by simply ringing a phone, that is, through a missed call. It detected the use of NSO Group's Pegasus spyware attacks through its applications on various devices.
17.05.2019	The Indian Computer Emergency Response Team (CERT-In), a Statutory body formed under the IT Act, 2000 confirmed WhatsApp's findings and published a vulnerability note on its website with the severity status 'High'. It explained that "Successful exploitation of this vulnerability could allow the attacker to access information on the system such as call logs, messages, photos, etc which could lead to further compromise of the system."
29.10.2019	WhatsApp Inc. filed a complaint in Federal Court in the United States, namely, the United States District Court of the Northern District of California against the NSO Group alleging that they sent malware termed 'Pegasus' using

	WhatsApp's system, to approximately 1,400 mobile phones and devices designed to infect those devices for the purpose of unlawful surveillance of the users of those phones and devices.
31.10.2019	The Indian Express published a news report to the effect that WhatsApp had revealed that at least two dozen journalists, academics, lawyers, and activists in India were contacted and alerted by WhatsApp that their phones had been under surveillance by Pegasus for a two-week period until May 2019
31.10.2019	The then Minister of Information and Technology, Shri Ravi Shankar Prasad released a statement on the micro-blogging platform twitter stating that the Government of India has asked WhatsApp to explain the kind of breach that occurred as per their vulnerability note; that Government agencies have a well-established protocol for interception which includes sanction and supervision from highly ranked officials in Central and State Governments for clear stated reasons and national interest; and that the Government of India is concerned about the privacy of Indian citizens.
01.11.2019	The Ministry of Electronics and Information Technology (MEITY), Respondent No. 2 herein, sent a notice to WhatsApp Inc. asking it to explain its reported breach in privacy in its application.

03.11.2019	WhatsApp Inc. responded to the notice sent by MEITY emphasising that it had already informed the Central Government that it had detected through its internal forensic audits that the devices of **121** Indians had been compromised by 'Pegasus' in May 2019 and early September of 2019.
19.11.2019	Shri Dayanidhi Maran, sitting Member of the Lower House of Parliament, raised an unstarred question number 351 in the Lok Sabha asking whether the Government of India was tapping WhatsApp calls and messages and whether protocols in getting permission for tapping WhatsApp calls were similar to that of mobile phones/ telephones. He also asked whether the Government uses the Israeli Software Pegasus for the same and the details thereof. On the same date, Minister of State, Ministry of Home affairs responded to the unstarred question by relying upon section 69 of the IT Act, 2000 and Section 5 of the Indian Telegraph Act, 1885 which empower the interception of messages in specified situations and emphasising that there was no blanket permission to any agency for interception, monitoring or decryption without permission of the competent Authority. However, the Minister did not answer the main query.
20.11.2019	A starred question submitted by Members of Parliament, Shri Asaduddin Owaisi and Shri Syed Imtiaz Jaleel, asked the Government of India, *inter alia*, "whether the

	Government has taken cognizance of the reports of alleged use and purchase of the Pegasus spyware by Government agencies and if so, the details thereof"? In response the then Union Minister of Electronics & Information Technology (MEITY), Shri Ravi Shankar Prasad submitted a written response stating that: "Yes, Sir. Government has taken note of the fact that a spyware/malware has affected some Whatsapp users. According to WhatsApp, this spyware was developed by an Israel based company NSO Group and that it had developed and used Pegasus spyware to attempt to reach mobile phones of a possible number of 1400 users globally that includes 121 users from India…On September 5, 2019 WhatsApp wrote to CERT-In mentioning an update to the security incident reported in May 2019, that while the full extent of this attack may never be known, WhatsApp continued to review the available information. It also mentioned that WhatsApp believes it is likely that devices of approximately one hundred and twenty one users in India may have been attempted to be reached. Based on media reports on 31st October, 2019, about such targeting of mobile devices of Indian citizens through WhatsApp by spyware Pegasus, CERT-In has issued a formal notice to WhatsApp seeking submission of relevant details and information."
28.11.2019	Pointed questions were raised to the then Union Minister of Electronics & Information Technology (MEITY), Shri

O

	Ravi Shankar Prasad on the use of Pegasus in India on the floor of the Rajya Sabha. In response to pointed questions from Members of Parliament, Shri Digvijaya Singh and Shri Jairam Ramesh as to whether the Government of India bought the Pegasus software, Shri Prasad said that all electronic interception of communications in India followed a standard operating procedure — and did not give a categorical denial to questions whether the Government of India or any of its agencies had bought the spyware. When Member of Parliament, Shri Anand Sharma pressed on the issue as to whether the Hon'ble Minister was aware of government-authorised surveillance, Shri Prasad said: "To the best of my knowledge, no unauthorised interception has been done
11.12.2019	Once again information was attempted to be sought from the Government of India in the form of unstarred questions was submitted by Shri. Mimi Chakraborty and Shri Anumula Revanth Reddy about whether: "WhatsApp was hacked to spy on Indian activists, Journalists and Lawyers and if so, the details thereof"; "the results of investigation conducted by the Government in this regard"; and "whether the Government has failed to check hacking of e-services in the country." Written responses were given by the Hon'ble Minister of State, MEITY, merely repeating the correspondence between CERT-In and WhatsApp Inc.

15.06.2020	Amnesty International and Citizen Lab uncovered another coordinated spyware campaign targeting nine human rights defenders in India. Some of these were already targeted with NSO Group's spyware in 2019.
02.02.2021	While hearing Writ Petition (Civil) No. 1038/2020 filed by Shri Binoy Viswam for personal data protection standards by the Reserve Bank of India and the National Payments Corporation of India, this Hon'ble Court enquired whether Pegasus has resulted in any mishap in India and directed the parties to file their respective affidavits. No affidavits were filed by the Union of India in this regard
24.03.2021	Members of Parliament, Dr. T. Sumathy (a) Thamizhachi Thangapandian: Shrimati Maneka Sanjay Gandhi, raised unstarred question number 4612 raising the following questions: "(a) whether the Government has found the presence of spywares or surveillance software such as pegases spyware the country and if so, the details thereof; and (b) whether the Government has launched any investigation into the presence, use and/or sale of spyware on surveillance software in the country and if so, the details thereof?" In response, Minister of State For Electronics And Information Technology, Shri Sanjay Dhotre submitted as follows: **"(a) and (b): There is no such information available with the Government."**
17.04.2021	CERT-In once again warned users of WhatsApp against

	vulnerabilities in the application noting that "Successful exploitation of these vulnerabilities could allow the attacker to execute arbitrary code or access sensitive information on a targeted system."
18.07.2021	A consortium of 17 journalistic organisations of long-standing repute across the globe released the results of a months long investigative report on the use of military grade spyware against journalists, political leaders, persons holding high constitutional office, doctors, public officials, survivors of sexual harassment, lawyers, human rights defenders, and ordinary citizens in several countries including India. The investigation and reporting are led by Paris based non-profit media organisation 'Forbidden Stories', and, Amnesty International, a Nobel Peace Prize winning international human rights organisation headquartered in London. Over 80 journalists from 40 countries participated in the consortium's investigations. Amongst the 37 forensically verified cases, Pegasus was detected on the phones of 10 Indian citizens. Forensic examination by cyber experts have confirmed the use of Pegasus infection in the phones of the following senior journalists: (i) S.N.M Abidi (Senior Journalist), (ii) Sushant Singh (Previously at Indian Express), (iii) M.K. Venu (Founder, The Wire), (iv) Siddharth Varadarajan (Founder, The Wire), and (v) Paranjoy Guha Thakurta (Senior Journalist). Attempts at hacking was detected on

	the phones of: (i) Vijaita Singh (Senior Journalist at The Hindu), (ii) Smita Sharma (Previously with TV18). The consortium investigated a leaked list of over 50,000 numbers, which were allegedly selected for surveillance by clients of the NSO Group. The reports state that the "list does not identify who put the numbers on it, or why, and it is unknown how many of the phones were targeted or surveilled. But forensic analysis of the 37 smartphones shows that many display a tight correlation between time stamps associated with a number on the list and the initiation of surveillance, in some cases as brief as a few seconds." Among 1500 verified numbers from this list, around 300 are Indian numbers of Indian citizens. This includes over 40 journalists. The list also includes major opposition figures, one constitutional authority, two serving ministers in the Government of India, current and former heads and officials of security organisations and scores of business persons. Most alarmingly, the list allegedly includes former Election Commissioner, Shri Ashok Lavasa. An unsigned and undated response was initially made available by ANI on 18.07.2021, ostensibly in response to queries by the Washington Post, and stated that "there has been no unauthorised interception by Government agencies". Shri Ashwini Vaishnaw, the present Union Minister of Electronics & Information Technology stated the same in the Parliament on 18.07.2021.

19.07.2021 till present	All attempts at seeking information and accountability in the Parliament of India have been stonewalled by the Government of India, in violation of citizen's right to know under Articles 19(1)(a) and 21 of the Constitution of India.
02.08.2021	Hence, this writ petition.

IN THE SUPREME COURT OF INDIA

(CIVIL ORIGINAL JURISDICTION)

PUBLIC INTEREST LITIGATION

WRIT PETITION (CIVIL) NO._____ OF 2021

(A petition under Article 32 of the Constitution of India praying for the issuance of a Writ of Mandamus or any other appropriate writ, direction or order for disclosure of information as to the violation of fundamental rights, abuse of power, and commission of criminal offences through use of electronic surveillance, hacking and spyware against Indian citizens; enforcement of the freedom of the press from interference through spying, hacking, and electronic surveillance; challenging the constitutional vires of Section 5 of the Indian Telegraph Act, 1885, Rule 419A of the Indian Telegraph Rules 1951, Section 69 of the Information Technology Act, 2000 and Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption) of Information Rules, 2009; and, for fair and impartial investigation by a special investigation team appointed and monitored by this Hon'ble Court)

IN THE MATTER OF:

1. **The Editors Guild of India**, [redacted]

…. **Petitioner No.1**

2. **Mrinal Pande,** [redacted]

…Petitioner No.2

Versus

1. **Union of India,** Through Principal Secretary, Ministry of Home Affairs, North Block, Raisina Hills, New Delhi, Delhi, 110001.

2. **Union of India,** Through Principal Secretary, Ministry of Electronics and Information Technology, Electronics Niketan, 6, CGO Complex, Lodhi Road, New Delhi - 110003.

3. **Union of India**, Through Principal Secretary, Ministry of Communications, Sanchar Bhawan, 20 Ashoka Road, New Delhi – 110001.

… Respondents

(All Respondents are Contesting Respondents)

WRIT PETITION UNDER ARTICLE 32 OF THE CONSTITUTION PRAYING FOR THE ISSUANCE OF A WRIT OF MANDAMUS OR ANY OTHER APPROPRIATE WRIT, DIRECTION OR ORDER UNDER ARTICLES 14, 19 AND 21 OF THE CONSTITUTION OF INDIA FOR DISCLOSURE OF INFORMATION AS TO THE

VIOLATION OF FUNDAMENTAL RIGHTS, ABUSE OF POWER, AND COMMISSION OF CRIMINAL OFFENCES THROUGH USE OF ELECTRONIC SURVEILLANCE, HACKING AND SPYWARE AGAINST INDIAN CITIZENS; ENFORCEMENT OF THE FREEDOM OF THE PRESS FROM INTERFERENCE THROUGH SPYING, HACKING, AND ELECTRONIC SURVEILLANCE; CHALLENGING THE CONSTITUTIONAL VIRES OF SECTION 5 OF THE INDIAN TELEGRAPH ACT, 1885, RULE 419A OF THE INDIAN TELEGRAPH RULES 1951, SECTION 69 OF THE INFORMATION TECHNOLOGY ACT, 2000 AND INFORMATION TECHNOLOGY (PROCEDURE AND SAFEGUARDS FOR INTERCEPTION, MONITORING AND DECRYPTION) OF INFORMATION RULES, 2009; AND FOR FAIR AND IMPARTIAL INVESTIGATION BY A SPECIAL INVESTIGATION TEAM APPOINTED AND MONITORED BY THIS HON'BLE COURT

To,

The Hon'ble the Chief Justice of India and His Companion Justices of the Supreme Court of India. The Writ Petition of the Petitioners above named

MOST RESPECTFULLY SHEWETH:

1. The present Writ Petition under Article 32 of the Constitution of India is being filed by the Petitioners seeking enforcement of the freedom of the press from interference through spying, hacking, and electronic surveillance; enforcement of the *right to know* on behalf of all citizens of India about the violation of fundamental rights, abuse of power, and commission of

criminal offences through use of electronic surveillance, hacking and spyware against Indian citizens; and challenging the constitutional vires of Section 5 of the Indian Telegraph Act, 1885, Rule 419A of the Indian Telegraph Rules 1951, Section 69 of the Information Technology Act, 2000 and Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption) of Information Rules, 2009. The petition further seeks a fair and impartial investigation by a special investigation team appointed and monitored by this Hon'ble Court.

ARRAY OF PARTIES

2. The Petitioner No.1 above-named is a society registered under the Societies Registration Act, 1860, which is an apex organization of Editors in India, was established in 1978 with the twin objectives of protecting freedom of the press, and raising the standards of editorial leadership of newspapers and magazines. Eminent editors of the day felt that the lack of an organized forum of editors was one of the reasons for the sustained suppression of press freedom during the Emergency. Since its inception, the Editors Guild has taken up issues of abuse of press freedom with the governments of the day, and has campaigned hard for protecting press freedom. Whether it is state lead persecution of journalists and media organisations, laws that curtail press freedom, or violence against journalists, the Guild has raised these issues with governments, both at national and state level, lead the public discourse through its statements and through member

publications, setup fact finding missions, and prepared reports that bring such issues to fore. Some of the most respected editors have been members of the Guild including, B G Verghese, Ajit Bhattacharjee, Nikhil Chakravarti, and Kuldip Nayyar. Currently, it has 200 editors from different geographies, mediums and languages as its members. Besides its elected office bearers led by Seema Mustafa, President, Sanjay Kapoor, General Secretary and Anant Nath, Treasurer, the Guild has eminent editors like N Ram, N Ravi, T N Ninan, Mrinal Pande, Coomi Kapoor, Shekhar Gupta, Raj Chengappa, K N Harikumar, Rajdeep Sardesai, and Naresh Fernandes amongst many of its active members. Therefore, the Guild represents the interests of journalists of all major print, television and digital news outlet in the country, especially with respect to the chilling impact of laws that curb media freedom on the work and livelihood of its members and journalists. As a professional guild it has responsibility and duty to take up these issues with the executive and when necessary, seek judicial intervention in order to ensure that there remains a conducive environment to carry on free and independent news reporting in the country, without fear or favour.

[redacted]

3. The Petitioner No.2 is a citizen of India and a journalist and author. Until 2009, she was the chief editor of the Hindi daily, *Hindustan*. In 2010 she was appointed as the chairperson of Prasar Bharti, the largest public broadcasting agency in India, created by an act of the Parliament and which controls the All India Radio and Doordarshan. She stepped down as the Chairperson of Prasar Bharti in 2012. The Petitioner No.2 is also a Padma Shri recipient, the fourth highest civilian honour. [redacted]

4. That the Petitioners do not have any personal interest or any personal gain or private motive or any other oblique reason in filing this Writ Petition in Public Interest. The Petitioners have not been involved in any other civil or criminal or revenue litigation, which could have legal nexus with the issues involved in the present Petition.

5. That the Petitioners in the present petition have not approached any other concerned authority in respect of the

issue involved in this present petition as this Hon'ble' Court is the constitutionally authorised forum where fundamental rights can be protected and enforced.

6. That Respondent No. 1 is the Union of India, represented by the Ministry of Home Affairs, which is the appropriate ministry dealing with questions of law and order, national security, and terrorism.

7. The Respondent No. 2 is the Union of India represented by the Ministry of Electronics and Information Technology, which is the appropriate ministry dealing with cyber-attacks and interception of computers, computer networks and electronic communications.

8. The Respondent No. 3 is the Union of India represented by the Ministry of Communications which is the appropriate ministry dealing with telecommunications.

FACTS OF THE CASE

9. The brief facts that give rise to the present Writ Petition are as follows:

10. After a long freedom struggle founded on principles of self-governance, justice, liberty, equality, fraternity and dignity, India obtained independence from colonial rule and became a democracy on August 15, 1947. This hard-won freedom was rendered sacrosanct through the adoption of the Constitution of India, a foundational charter of the Republic of India to ensure that the sovereign power of the people would never again be snatched away.

11. The Constitution of India brought into effect a system of limited government, transforming the political system in India from a culture of rule by authority to a *culture of justification*: a legal and political culture in which "every exercise of power is expected to be justified; in which the leadership given by government rests on the cogency of the case offered in defence of its decisions, not the fear inspired by the force at its command."[1]

12. The enforcement of fundamental rights by constitutional courts is a central pillar for this new culture of justification under the Constitution. In this conception, rights are not merely bright-line boundaries between the spheres of individual freedom and legitimate state power, but rather constitute a social and political practice. They are standards for deliberation on vital socio-political issues. In addition to issuing writs, this Hon'ble Court has the hallowed role of enforcing fundamental rights through a "bounded-deliberative" approach whereby public officials are called upon to publicly explain and justify their actions/inactions. [Judgement of this Hon'ble Court dated 30.04.2021 in Suo Motu Writ Petition (Civil) No.3 of 2021, at paragraph 5]

13. A culture of justification relies on zealous and uninhibited interrogation of state action. In the social and political practice of deliberative democracy, the freedom of the press, the free flow of information and a thriving market place of ideas provide the supporting structure for public deliberation.

---

[1] Etinenne Mureinik, *A Bridge to Where? Introducing the Interim Bill of Rights*, 10 S. AFR. J. HUM. RTS. 31 (1994).

Journalists perform a vital role in this system by providing information to the public and advancing public reason.

LAW ON INTERCEPTION

14. Judicial oversight over use of law-and-order powers of the state is an important means of limiting governmental authority. While integral to the social contract in terms of safeguarding all persons from harm and enforcing Rule of Law, policing must be exercised within the bounds of constitutional authority. The use of technologies for interception of communications between persons has been an arena of law-and-order that necessarily attracts heightened scrutiny because of its invasive and corrosive impact on privacy and fundamental freedoms in our democracy.

15. On 18.12.1996, this Hon'ble Court delivered a landmark judgement in the case of ***PUCL v. Union of India***, reported in (1997) 1 SCC 301, on interception of telecommunications under the Indian Telegraph Act, 1885. A pre-constitutional statute, the Indian Telegraph Act, 1885 had broad sweeping powers of interception to facilitate the autocratic schemes of the erstwhile colonial rulers. In this case, this Hon'ble Court held that the right to privacy is a part of the right to life and personal liberty under Article 21 of the Constitution of India. Any procedure under law authorising phone tapping must be just, fair and reasonable and not unreasonably infringe upon the right to privacy. In the absence of rules under the legislation, this Hon'ble Court laid down a procedure to be followed for lawful targeted surveillance of telecommunications. These include preconditions of public

emergency or public safety, a prior written order by the lawfully designated authority, review of these orders, expiry date for such orders, basic assessment of necessity and proportionality (whether other reasonable means to obtain the information are available), principle of least privilege, use limitation, and confidential record keeping. These guidelines, however, were designed keeping in mind telephone communications as they were in 1996. They were also meant to be a temporary, minimum standards, while Parliament could institute more comprehensive and forward-looking procedures for interception orders.

16. The onset of the internet revolution brought unique innovations and challenges for all spheres of human civilisation, including law and order. To meet these new challenges, and pursuant to the adoption of the Model Law on Electronic Commerce by the United Nations Commission on International Trade Law, vide General Assembly of the United Nations Resolution A/RES/51/162, dated 30th January, 1997, the Information Technology Act, 2000 was passed by the Indian Parliament in 2000 (hereinafter referred to as the "**IT Act, 2000**"). The legislation came into force on 17.10.2000 and became the Indian law governing the use of electronic communication devices, computers and computer systems amongst other systems.

17. The IT Act, 2000 comprehensively regulates all nature of activities and communications on electronic communication devices, computers, computer networks, computer resources and computer systems. This includes prohibiting accessing,

copying, extracting, contaminating, damaging, disrupting, altering, stealing from, and blocking access to any computer, computer system or computer network, without permission from the owner/person in charge [Section 43 and 66]. Also prohibited is fraudulent or dishonest use of passwords [Section 66C]; capture/publishing/transmitting images of private areas of a person without her consent [Section 66E]; cyber-terrorism [Section 66F]; and breach of confidentiality and privacy [Section 72]. These statutory provisions use civil and criminal law remedies to implement the fundamental rights to privacy, bodily integrity, dignity and freedom of speech and expression under Articles 19 and 21 of the Constitution of India.

18. Section 69 of the IT Act, 2000 as it was originally framed in the year 2000, authorised the **'Controller'** appointed under the Act to, by order, direct any agency of the Government to intercept any information transmitted through any computer resource, if she is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing.

19. On 01.03.2007, a decade after the guidelines in ***PUCL v. Union of India (supra)*** were laid down, the Indian Telegraph (Amendment) Rules, 2007 were notified. These rules inserted Rules 419A into the Indian Telegraph Rules, 1951, which instituted a procedure for interception of telecommunications.

Rule 419A comprises a modified version of the ***PUCL v. Union of India (supra)*** guidelines with allowances for *post facto* interception orders for "operational reasons" or in "remote locations", amongst other flexibilities. Despite the substantial leaps in technology since 1996, no special protections were instituted for the expanded quantity and quality of sensitive personal information now stored and conveyed on phones. The overlaps between electronic communication and telecommunication were also not examined.

20. On 27.10.2009, the Information Technology (Amendment) Act, 2008 (Act No. 10 of 2009) was brought into force. This substituted the erstwhile Section 69 of the IT Act, 2000 with a completely new provision that empowered the Central and State governments to authorise interception, monitoring or decryption of information on a computer resource. The new Section 69 reads as follows:

> "(1) Where the Central Government or a State Government or any of its officer specially authorised by the Central Government or the State Government, as the case may be, in this behalf may, if satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource.

> (2) The procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed.
> (3) The subscriber or intermediary or any person in-charge of the computer resource shall, when called upon by any agency referred to in sub-section (1), extend all facilities and technical assistance to-
> (a) provide access to or secure access to the computer resource generating transmitting, receiving or storing such information; or
> (b) intercept, monitor, or decrypt the information, as the case may be; or
> (c) provide information stored in computer resource.
> (4) The subscriber or intermediary or any person who fails to assist the agency referred to in sub-section (3) shall be punished with imprisonment for a term which may extend to seven years and shall also be liable to fine."

21. On the same date, i.e., 27.10.2009, the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption) of Information Rules, 2009 came into force and provided the procedure to be followed for the interception, monitoring and decryption of information stored in or transmitted by electronic devices and computers in India under Section 69 of the IT Act, 2000 (hereinafter referred to as the "**IT Interception Rules, 2009**").

22. The standards in ***PUCL v. Union of India*** **(supra)** and its application in Rule 419A of the Indian Telegraph Rules, 1951 and the IT Interception Rules, 2009 fail to protect the right to freedom of speech and expression, the right to privacy, and due process of law under the Constitution of India. They do not authorise hacking or infecting electronic devices with malware that allows complete takeover of the device.

23. These rules reflect the level of risk to privacy as contemplated by the technology of the time. These rules could not anticipate and do not authorise the exponential expansion in surveillance and hacking capabilities since their introduction. This is reflected, for example, in the rules framed for time periods of surveillance (which is redundant in present day smart phones since a single second of hacking can access years' worth of data), record keeping, destroying of records, authorisation to executive officials and absence of judicial oversight. In light of the recent exponential leaps in technology and collection of personal data, these standards do not adequately safeguard the freedom of the press, freedom of speech and expression, and the right to privacy.

24. Technological advances have meant that phones have become gateways to almost every facet of a person's life. Individual phones store unprecedented treasure troves of sensitive personal information. This includes intimate correspondence, emails, photographs, banking and other financial data, health information, bodily activity records (including second by second cataloguing of heart rate, menstrual logs, etc.), biometrics, GPS location, internet search history, shopping history and so on. This expansion in the quality and quantity of intimate and sensitive personal information on our phones and other electronic devices necessitates the evolving of new standards for access to these devices. Prior judicial orders by issuing a warrant for search or seizure pursuant to an investigation would be a precondition for the state to access many categories of such information. These protections are

only strengthened by recent developments in the law of privacy.

25. On 24.08.2017 a nine-judge bench of this Hon'ble Court unanimously affirmed that the right to privacy is a fundamental right guaranteed by the Constitution of India in the case of ***K.S. Puttaswamy v Union of India*** reported in (2017) 10 SCC 1 thereby guaranteeing to citizens the right to live life with privacy and personal dignity. Privacy was held to include informational privacy and bodily privacy, and incorporate notions of choice, autonomy, and consent.

26. On 20.12.2018, vide Notification bearing S.O. 6227(E), the Union of India authorised 10 of its agencies under Rule 4 of the IT Interception Rules, 2009 for the purposes of interception, monitoring and decryption of any information generated, transmitted, received or stored in any computer resource as contemplated by Section 69 of the IT Act, 2000.

A copy of Notification S.O. 6227(E) dated 20.12.2018 is annexed herewith and marked as **Annexure P-3 [Page 76 to 77).**

27. On 26.09.2018, a Constitution Bench of this Hon'ble Court delivered the decision in ***K.S. Puttaswamy v Union of India (II)(Aadhaar)***, reported in (2019) 1 SCC 1, reaffirming the test for proportionality review laid down in ***Puttaswamy (supra)***.

28. Following the decision in ***Puttaswamy (supra)***, and ***K.S. Puttaswamy v Union of India (II)(Aadhaar) (supra)***, the constitutional vires of Section 69 of the IT Act, 2000; the IT Interception Rules, 2009, and the Notification S.O. 6227(E)

dated 20.12.2018 were challenged before this Hon'ble Court in Writ Petition (Civil) No. 44 of 2019 (tagged with others) in which this Hon'ble Court was pleased to issue notice on 14.01.2019. These provisions, along with Rule 419A of the Indian Telegraph Rules, 1951 were also challenged in Writ Petition (Civil) No. 61 of 2019 in which this Hon'ble Court was pleased to issue notice on 25.01.2019.

A copy of Order dated 14.01.2019 in Writ Petition (Civil) No. 44 of 2019 is annexed herewith and marked as **Annexure P- 4 [Page 78 to 79)**

A copy of Order dated 25.01.2019 in Writ Petition (Civil) No. 61 of 2019 is annexed herewith and marked as **Annexure P- 5 [Page 80]**

LAW ON PRESS FREEDOM AND PUBLIC ACCOUNTABILITY

29. The freedom of speech and expression under Article 19(1)(a) of the Constitution of India includes the freedom of the press. This has been a long-standing principle propounded by this Hon'ble Court from as early as the decision in ***Brij Bhushan v. State of Delhi*****,** reported in AIR 1950 SC 129. The freedom of the press has been recognised as both necessary for and including holding the government accountable for its actions and policies.

30. In ***Bennett Coleman & Co. v. Union of India***, reported in (1972) 2 SCC 788, Hon'ble A. N. RAY J. (as he then was), speaking for the majority observed the importance of freedom

of the press for public accountability, calling it the 'Ark of the Covenant' in every democracy.

> "**80**. The faith of a citizen is that political wisdom and virtue will sustain themselves in the free market of ideas so long as the channels of communication are left open. The faith in the popular Government rests on the old dictum, "let the people have the truth and the freedom to discuss it and all will go well." The liberty of the press remains an "Ark of the Covenant" in every democracy."

Hon'ble H. M. BEG J., in his concurring opinion, echoed this observing that:

> "Freedom of the Press is the Ark of the Covenant of Democracy because public criticism is essential to the working of its institutions."

31. In ***Indian Express Newspapers (Bombay) (P) Ltd. v. Union of India*****,** reported in (1985) 1 SCC 641, this Hon'ble Court speaking through Hon'ble VENKATARAMIAH J. freedom of press means freedom from interference which would affect journalistic reporting:

> "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. … 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.
> …
> "84. Freedom of press as the petitioners rightly assert means freedom from interference from authority which would have the effect of interference with the content and circulation of newspapers."

32. In ***The Printers (Mysore) Ltd. v. CTO***, reported in (1994) 2 SCC 434, this Hon'ble Court speaking through Hon'ble JEEVAN REDDY J. held that freedom of the press would mean bringing to the fore the misdeeds of the government:

> "13. Freedom of press has always been a cherished right in all democratic countries. The newspapers not only purvey news but also ideas, opinions and ideologies besides much else. They are supposed to guard public interest by bringing to fore the misdeeds, failings and lapses of the Government and other bodies exercising governing power. Rightly, therefore, it has been described as the Fourth Estate. The democratic credentials of a State are judged today by the extent of freedom the press enjoys in that State."

33. This Hon'ble Court has resisted attempts to intimidate and muzzle accountability by the free press through use of law-and-order powers of the state. In Judgement dated 03.06.2021 in Writ Petition (Criminal) No. 154 of 2020 titled "Vinod Dua v. State of" this Hon'ble Court quashed an FIR alleging the commission of, *inter alia,* the offence of sedition against a journalist on the ground of his reporting on failures of the state. While quashing the FIR, this Hon'ble Court observed that the prosecution "would be unjust" and "violative of the rights of the petitioner guaranteed under Article 19(1)(a) of the Constitution."

EVENTS LEADING TO THE PRESENT PETITION

34. On 18.09.2018, Citizen Lab, an interdisciplinary laboratory based at the prestigious Munk School of Global Affairs and Public Policy, University of Toronto, Canada, published a

research report to the effect that an Israeli cyber-warfare vendor "NSO Group" had produced and is selling a mobile spyware suite named 'Pegasus' for invasive (including trans-border) surveillance against individuals. Citizen Lab found suspected Pegasus infections in 45 countries: Algeria, Bahrain, Bangladesh, Brazil, Canada, Cote d'Ivoire, Egypt, France, Greece, **India**, Iraq, Israel, Jordan, Kazakhstan, Kenya, Kuwait, Kyrgyzstan, Latvia, Lebanon, Libya, Mexico, Morocco, the Netherlands, Oman, Pakistan, Palestine, Poland, Qatar, Rwanda, Saudi Arabia, Singapore, South Africa, Switzerland, Tajikistan, Thailand, Togo, Tunisia, Turkey, the UAE, Uganda, the United Kingdom, the United States, Uzbekistan, Yemen, and Zambia. Despite these shocking revelations, no public investigations were conducted to unveil the perpetrators and scope of these cyber attacks on Indian citizens.

A copy of the report with citation, Bill Marczak, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ron Deibert. "Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries," Citizen Lab Research Report No. 113, University of Toronto, September 2018 is annexed herewith and marked as **Annexure P- 6 [Page 81 to 120]**

<u>NSO Group</u>

35. The "NSO Group" is an Israeli company which specialises in creating military grade cyber weapons. Pegasus is one of its products that has astronomical surveillance and hacking capabilities. It operates as a 'malware' that infects electronic

devices and spies on the victim by transferring data to a master server in an unauthorised manner. Pegasus is capable of a range of spyware operations from accessing every bit of stored data on one's phone to real time access to emails, texts, phone calls, to controlling all cameras on the device, to activating the sound recording function, to transmitting all sounds in the vicinity of the device, to detecting whether two phones have come in physical proximity. This means that Pegasus can listen in on your calls, view your messages, see your pictures, record calls, know your every movement, know who you came in physical proximity with, know your internet use history, know your banking information, know your health information and more. Pegasus is an extremely sophisticated spyware which can go undetected, except by very skilled cyber forensic analysis.

A copy of news report dated 18.07.2021 titled *"What is Pegasus spyware and how does it hack phones?"* published by The Guardian, available at url https://www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones is annexed herewith and marked as **Annexure P- 7 [Page 121 to 125]**

36. Pegasus' capabilities far exceed any notion of interception or monitoring of communications. By infecting the targeted device, Pegasus hands over control of the device to the hacker, who can then access every feature on the device, including when it is switched off. The access to continuous location data is tantamount to wearing of an ankle GPS bracelet, which is a punitive action awarded by courts after

commission of an offence, and not a mere investigative tool. The access to voice samples stored on the device would otherwise require an order from a court. The access to bodily measurements (including finger-prints) can only be collected on arrest after registration of an FIR. The access to health records, banking records, business records, etc. can only be summoned or seized pursuant to an on-going investigation or trial, with warrant (and without warrant in exceptional cases). Materials that could tend to incriminate a person are prohibited from forceful disclosure. Thus, it is submitted that Pegasus is a spyware "suite" that far exceeds mere interception or monitoring of communications.

37. Most crucially, the NSO Group states that its products are "**used exclusively by government intelligence and law enforcement agencies**.'

A copy of 'About Us' on NSO Group's website at url <https://www.nsogroup.com/about-us/> is annexed herewith and marked as **Annexure P- 8 [Page 126 to 130]**

<u>Pegasus Attacks</u>

38. In May 2019, WhatsApp Inc. identified a vulnerability in its phone application which allowed attackers to inject spyware in the targets software by simply ringing a phone, that is, through a missed call. It detected the use of NSO Group's Pegasus spyware through its applications on various devices.

A copy of news report dated 14.05.2019 titled *"WhatsApp voice calls used to inject Israeli spyware on phones,"* published by The Financial Times, available at url https://www.ft.com/content/4da1117e-756c-11e9-be7d-

6d846537acab is annexed herewith and marked as **Annexure P-9 [Page 131 to 134]**

39. On 17.05.2019 the Indian Computer Emergency Response Team (CERT-In) a Statutory body formed under the IT Act, 2000 confirmed WhatsApp's findings and published a vulnerability note on its website with the severity status 'High'. This vulnerability note states as follows:

> "Overview: A vulnerability has been reported in WhatsApp which could be exploited by a remote attacker to execute arbitrary code on the affected system.
> Description: This vulnerability exists in WhatsApp due to a buffer overflow condition error. A remote attacker could exploit this vulnerability by making a decoy Whatsapp voice call to a target user's phone number and thereby sending specially crafted series of SRTCP packets to the target system. This could trigger a buffer overflow condition leading to execution of arbitrary code by the attacker.
> Successful exploitation of this vulnerability could allow the attacker to access information on the system such as call logs, messages, photos, etc which could lead to further compromise of the system."

A copy of the CERT-In vulnerability note dated 17.05.2019 available at <https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES01&VLCODE=CIVN-2019-0080> is annexed herein and marked as **Annexure P- 10 [Page 135 – 136]**

40. On 29.10.2019, WhatsApp Inc. filed a complaint in Federal Court in the United States, namely, the United States District Court of the Northern District of California against the NSO Group alleging that they sent malware termed 'Pegasus' using WhatsApp's system, to approximately 1,400 mobile phones and devices designed to infect those devices for the purpose of unlawful surveillance of the users of those phones and devices. On 16.07.2020, the Federal Court denied NSO Groups' 'motion to dismiss' the complaint, whereby the case will next proceed to trial.

A copy of the Judgement dated 16.07.2020 issued by the United States District Court of the Northern District of California in Case No. 19cv-07123-PJH titled "WhatsApp Inc. et.al. v. NSO Group Technologies et. al." is annexed herewith and marked as **Annexure P- 11 [Page 137 to 181].**

41. On 31.10.2019, the Indian Express published a news report to the effect that WhatsApp had revealed that at least two dozen journalists, academics, lawyers, and activists in India were contacted and alerted by WhatsApp that their phones had been under surveillance by Pegasus for a two-week period until May 2019.

A copy of the news report dated 31.10.2019, titled "*WhatsApp confirms: Israeli spyware was used to snoop on Indian journalists, activists*," published by the Indian Express, available at url < https://indianexpress.com/article/india/whatsapp-confirms-israeli-spyware-used-snoop-on-indian-journalists-activists-pegasus-facebook-6095296/> is annexed herewith and marked as **Annexure P- 12 [Page 182 to 192]**

Government of India's response

42. On 31.10.2019 the then Minister of Information and Technology, Shri Ravi Shankar Prasad released a statement on the micro-blogging platform twitter stating that the Government of India is concerned about the breach of privacy of citizens of India on the messaging platform WhatsApp. He further stated that the Government of India has asked WhatsApp to explain the kind of breach that occurred as per their vulnerability note. He also stated that the Government of

India is committed to protect the privacy of all Indian Citizens. He further stated that Government agencies have a well-established protocol for interception which includes sanction and supervision from highly ranked officials in Central and State Governments for clear stated reasons and national interest.

A copy of the statement dated 31.10.2019 published by @rsprasad handle on twitter at url <https://twitter.com/rsprasad/status/1189867398662213632?lang=en> is annexed herewith and marked as **Annexure P-13 [Page 193]**

43. On 01.11.2019, the Ministry of Electronics and Information Technology (MEITY), Respondent No. 2 herein, sent a notice to WhatsApp Inc. asking it to explain its reported breach in privacy in its application. On 03.11.2019, WhatsApp Inc. responded to the notice sent by MEITY emphasising that it had already informed the Central Government that it had detected through its internal forensic audits that the devices of **121** Indians had been compromised by 'Pegasus' in May 2019 and early September of 2019.

A copy of the news report dated 03.11.2019 titled "*Besides May alert, WhatsApp sent another in September on 121 Indians breached,"* published by the Indian Express, available at url <https://indianexpress.com/article/india/besides-may-alert-whatsapp-sent-another-in-sept-on-121-indians-breached-6100265/> is annexed herewith and marked as **Annexure P-14 [Page 194 to 205]**

A copy of the news report dated 03.11.2019 titled *"Alerted Indian govt. of spyware attack in September, says WhatsApp"* published by The Hindu, available at url <https://www.thehindu.com/news/national/alerted-indian-govt-of-spyware-attack-in-sept-whatsapp/article29870449.ece> is annexed herewith and marked as **Annexure P- 15 [Page 206 to 209]**

44. On 19.11.2019, Shri Dayanidhi Maran, sitting Member of the Lower House of Parliament, raised an unstarred question number 351 in the Lok Sabha asking whether the Government of India was tapping WhatsApp calls and messages and whether protocols in getting permission for tapping WhatsApp calls were similar to that of mobile phones/ telephones. He also asked whether the Government uses the Israeli Software Pegasus for the same and the details thereof. On the same date, Minister of State, Ministry of Home affairs responded to the unstarred question by relying upon section 69 of the IT Act, 2000 and Section 5 of the Indian Telegraph Act, 1885 which empower the interception of messages in specified situations and emphasising that there was no blanket permission to any agency for interception, monitoring or decryption without permission of the competent Authority. However, the Minister did not answer the main query.

A copy of the unstarred question number 351 along with its response in the Lok Sabha is annexed herewith and marked as **Annexure P - 16 [Page 210 to 212].**

45. On 20.11.2019, a starred question submitted by Members of Parliament, Shri Asaduddin Owaisi and Shri Syed Imtiaz

Jaleel, asked the Government of India, *inter alia*, "whether the Government has taken cognizance of the reports of alleged use and purchase of the Pegasus spyware by Government agencies and if so, the details thereof"? In response the then Union Minister of Electronics & Information Technology (MEITY), Shri Ravi Shankar Prasad submitted a written response stating that:

> "(a), (b) and (c) : Yes, Sir. Government has taken note of the fact that a spyware/malware has affected some Whatsapp users. According to WhatsApp, this spyware was developed by an Israel based company NSO Group and that it had developed and used Pegasus spyware to attempt to reach mobile phones of a possible number of 1400 users globally that includes 121 users from India.
> (d) : Some statements have appeared, based on reports in media, regarding this. These attempts to malign the Government of India for the reported breach are completely misleading. The Government is committed to protect the fundamental rights of citizens, including the right to privacy. The Government operates strictly as per provisions of law and laid down protocols. There are adequate provisions in the Information Technology (IT) Act, 2000 to deal with hacking, spyware etc.
> (e) and (f) : The Indian Computer Emergency Response Team (CERT-In) published a vulnerability note on May 17, 2019 advising countermeasures to users regarding a vulnerability in WhatsApp. Subsequently, on May 20, 2019 WhatsApp reported an incident to the CERT-In stating that WhatsApp had identified and promptly fixed a vulnerability that could enable an attacker to insert and execute code on mobile devices and that the vulnerability can no longer be exploited to carry out attacks. On September 5, 2019 WhatsApp wrote to CERT-In mentioning an update to the security incident reported in May 2019, that while the full extent of this attack may never be known, WhatsApp continued to review the available information. It also mentioned that WhatsApp believes it is likely that devices of approximately one hundred and twenty one users in India may have been attempted to be reached. Based on media reports on 31st October, 2019, about such targeting of mobile devices of Indian citizens through WhatsApp by spyware Pegasus, CERT-In has issued a formal notice to WhatsApp seeking submission of relevant details and information.

(g) : Ministry of Electronics & Information Technology is working on the Personal Data Protection Bill to safeguard the privacy of citizens, and it is proposed to table it in Parliament."

A copy of starred question number *47 along with answer dated 20.11.2019 is annexed herewith and marked as **Annexure P - 17 [Page 213 to 214].**

46. On 28.11.2019, pointed questions were raised to the then Union Minister of Electronics & Information Technology (MEITY), Shri Ravi Shankar Prasad on the use of Pegasus in India on the floor of the Rajya Sabha. In response to pointed questions from Members of Parliament, Shri Digvijaya Singh and Shri Jairam Ramesh as to whether the Government of India bought the Pegasus software, Shri Prasad said that all electronic interception of communications in India followed a standard operating procedure and did not give a categorical denial to questions whether the Government of India or any of its agencies had bought the spyware. When Member of Parliament, Shri Anand Sharma pressed on the issue as to whether the Hon'ble Minister was aware of government-authorised surveillance, Shri Prasad said: "To the best of my knowledge, no unauthorised interception has been done."

47. On 11.12.2019, once again information was attempted to be sought from the Government of India in the form of unstarred questions was submitted by Shri. Mimi Chakraborty and Shri Anumula Revanth Reddy about whether: "WhatsApp was hacked to spy on Indian activists, Journalists and Lawyers and if so, the details thereof"; "the results of investigation conducted by the Government in this regard"; and "whether the Government has failed to check hacking of e-services in the country." Written responses were given by the Hon'ble

Minister of State, MEITY, merely repeating the correspondence between CERT-In and WhatsApp Inc.

A copy of unstarred question number 3686 answered on 11.12.2019 in the Lok Sabha is annexed herewith and marked as **Annexure P – 18 [Page 215 to 216].**

A copy of unstarred question number 3785 answered on 11.12.2019 in the Lok Sabha is annexed herewith and marked as **Annexure P - 19 [Page 217 to 218]**

48. On 15.06.2020 Amnesty International and Citizen Lab uncovered another coordinated spyware campaign targeting nine human rights defenders in India. Some of these were already targeted with NSO Group's spyware in 2019.

A copy of the report dated 15.06.2020 titled *"India: Human Rights Defenders Targeted by a Coordinated Spyware Operation,"* published by Amnesty International and Citizen Lab, available at url <https://www.amnesty.org/en/latest/research/2020/06/india-human-rights-defenders-targeted-by-a-coordinated-spyware-operation/> is annexed herewith and marked as **Annexure P - 20 [Page 219 to 235].**

49. On 02.02.2021, while hearing Writ Petition (Civil) No. 1038/2020 filed by Shri Binoy Viswam for personal data protection standards by the Reserve Bank of India and the National Payments Corporation of India, this Hon'ble Court enquired whether Pegasus has resulted in any mishap in India and directed the parties to file their respective affidavits. No affidavits were filed by the Union of India in this regard.

50. On 24.03.2021, Members of Parliament, Dr. T. Sumathy (a) Thamizhachi Thangapandian: Shrimati Maneka Sanjay Gandhi, raised unstarred question number 4612 raising the following questions: "(a) whether the Government has found the presence of spywares or surveillance software such as pegases spyware the country and if so, the details thereof; and (b) whether the Government has launched any investigation into the presence, use and/or sale of spyware on surveillance software in the country and if so, the details thereof?" In response, Minister of State For Electronics And Information Technology, Shri Sanjay Dhotre submitted as follows: **"(a) and (b): There is no such information available with the Government."**

A copy of the unstarred question number 4612 along with its response in the Lok Sabha is annexed herewith and marked as **Annexure P - 21 [Page 236]**

51. On 17.04.2021 the Indian Computer Emergency Response Team (CERT-In) once again warned users of WhatsApp against vulnerabilities in the application noting that "Successful exploitation of these vulnerabilities could allow the attacker to execute arbitrary code or access sensitive information on a targeted system."

A copy of the CERT-In vulnerability note dated 12.04.2021 available on url <https://cert-in.org.in/> is annexed herewith and marked as **Annexure P - 22 [Page 237]**

JULY 2021 INVESTIGATIVE REPORTS

52. On 18.07.2021, a consortium of 17 journalistic organisations of long-standing repute across the globe released the results of a months long investigative report on the use of military grade spyware against journalists, political leaders, persons holding high constitutional office, doctors, public officials, survivors of sexual harassment, lawyers, human rights defenders, and ordinary citizens in several countries including India. The investigation and reporting are led by Paris based non-profit media organisation 'Forbidden Stories', and, Amnesty International, a Nobel Peace Prize winning international human rights organisation headquartered in London. Over 80 journalists from 40 countries participated in the consortium's investigations.

A copy of journalistic report dated 18.07.2021 titled *"Private Israeli spyware used to hack cellphones of journalists, activists worldwide,"* published by the Washington Post, available at <https://www.washingtonpost.com/investigations/interactive/2021/nso-spyware-pegasus-cellphones/> is annexed herewith and marked as **Annexure P- 23 [Pages 238 to 257].**

53. These investigations uncovered that Pegasus was detected to have been used on several electronic communication devices, such as smart phones, that were forensically examined by experts (hereinafter referred to as "the Pegasus cyber attacks"). Amongst the 37 forensically verified cases, Pegasus was detected on the phones of 10 Indian citizens. The

consortium investigated a leaked list of over 50,000 numbers, which were allegedly selected for surveillance by clients of the NSO Group. The reports state that the "list does not identify who put the numbers on it, or why, and it is unknown how many of the phones were targeted or surveilled. But forensic analysis of the 37 smartphones shows that many display a tight correlation between time stamps associated with a number on the list and the initiation of surveillance, in some cases as brief as a few seconds."

54. The report alleges that forensic analysis detected that Pegasus was installed on phones, *inter alia*, through a "zero-click process": it does not require any action by the targeted phone's user, and can remotely infiltrate a device with the help of spyware/malware. Pegasus delivers a chain of "zero-day exploits" to penetrate security features on the phone and installs Pegasus without the user's knowledge or permission. A zero-day exploit is a completely unknown vulnerability, about which even the software manufacturer is not aware, and there is, thus, no patch or fix available for it. Its exclusive nature makes Pegasus a highly effective and expensive tool for usage. Pegasus can also only be detected by highly skilled technical forensic methods, and regular anti-virus software is unable to detect it. As exploits get discovered and vulnerabilities are fixed, the NSO Group develops and integrates newer and more advanced mechanisms for delivering and hiding Pegasus on devices.

55. Forensic examination by cyber experts have confirmed the use of Pegasus infection in the phones of the following senior

journalists: (i) S.N.M Abidi (Senior Journalist), (ii) Sushant Singh (Previously at Indian Express), (iii) M.K. Venu (Founder, The Wire), (iv) Siddharth Varadarajan (Founder, The Wire), and (v) Paranjoy Guha Thakurta (Senior Journalist). Attempts at hacking were detected on the phones of: (i) Vijaita Singh (Senior Journalist at The Hindu), (ii) Smita Sharma (Previously with TV18).

A copy of journalistic report dated 18.07.2021 titled *"Pegasus Project: How Phones of Journalists, Ministers, Activists May Have Been Used to Spy On Them,"* published by the Wire, available at url <https://thewire.in/government/project-pegasus-journalists-ministers-activists-phones-spying> is annexed herewith and marked as **Annexure P- 24 [Pages 258 to 268].**

56. At least 300 Indian citizens are present on the list of potentially targeted persons uncovered by the consortium. This allegedly includes over 40 journalists, major opposition figures, one constitutional authority, two serving ministers in the Government of India, current and former heads and officials of security organisations and scores of business persons. The journalists on the list include:

- Shishir Gupta: Executive editor at Hindustan Times
- Rohini Singh: Freelance journalist who has written several exposes for The Wire about controversial business dealings of politicians or their family members.
- Devirupa Mitra: The Wire's diplomatic editor.
- Prashant Jha: Views editor of Hindustan Times, formerly the bureau chief.

- Prem Shankar Jha: A veteran journalist who held editorial positions at Hindustan Times, the Times of India and several other newspapers. He is a regular contributor to The Wire.
- Swati Chaturvedi: Freelance journalist who has contributed to The Wire and author of the book *I Am A Troll: Inside the Secret World of the BJP's Digital Army* (New Delhi: Juggernaut Publication, 2016).
- Rahul Singh: Defence correspondent for Hindustan Times.
- Aurangzeb Naqshbandi: A political reporter who formerly worked for Hindustan Times and covered the Congress party.
- Ritika Chopra: A journalist for the Indian Express who covers the education and Election Commission beats.
- Muzamil Jaleel: Another Indian Express journalist who covers Kashmir.
- Sandeep Unnithan: India Today journalist who reports on defence and the Indian military.
- Manoj Gupta: Editor of investigations and security affairs at TV18.
- J. Gopikrishnan: An investigative reporter with The Pioneer, he broke the 2G telecom scam.
- Saikat Datta: Formerly a national security reporter.
- Ifthikar Gilani: Former DNA reporter who reports on Kashmir.
- Manoranjan Gupta: Northeast-based editor in chief of Frontier TV.
- Sanjay Shyam: A Bihar-based journalist.
- Jaspal Singh Heran: An octogenarian who is the editor-in-chief of the Ludhiana-based Punjabi daily Rozana Pehredar.
- Roopesh Kumar Singh: A freelance based in Jharkhand's Ramgarh.
- Deepak Gidwani: Former correspondent of DNA, Lucknow.
- Sumir Kaul: A journalist for news agency PTI.
- Shabir Hussain: A Delhi-based political commentator from Kashmir.

57. Most alarmingly, the list allegedly includes former Election Commissioner, Shri Ashok Lavasa. The list also allegedly includes several members of the Opposition including, Shri Rahul Gandhi of the Indian National Congress and two of his aides, Shri Abhishek Bannerjee of the Trinamool Congress Party, Shri Prashant Kishor (political analyst) who has

worked with Opposition Parties, Shri G. Parameshwara (Deputy chief minister in the JD(S)-Congress coalition government in Karnataka, which was toppled after several MLAs defected to the BJP), Shri Satish (Personal secretary to Shri H.D. Kumaraswamy, who was chief minister of Karnataka, Shri Venkatesh (Personal secretary to Shri Siddaramaiah, who was the Congress chief minister of Karnataka before Shri H. D Kumaraswamy).

A copy of journalistic report dated 27.07.2021 titled *"Pegasus Project: 155 Names Revealed By The Wire On Snoop List So Far,"* published by the Wire, available at url <https://thewire.in/rights/project-pegasus-list-of-names-uncovered-spyware-surveillance> is annexed herewith and marked as **Annexure P- 25 [Pages 269 to 293].**

58. The investigative reports also revealed the use of spyware to harass, intimate and sexually exploit women working as journalists. For example, Ghada Oueiss, a Lebanese broadcast journalist at Al-Jazeera, had photographs of her taken in private scenarios posted on the internet, with salacious commentary that was demeaning to her personal dignity. Several Indian women who work as journalists are present on the list of potential victims of hacking raising severe concerns about the use of hacking of cameras to invade their privacy and commit gendered crimes against them.

A copy of journalistic report dated 01.08.2021, titled *"'I will not be silenced': Women targeted in hack-and-leak attacks speak out about spyware*" published by NBW News, available at https://www.nbcnews.com/tech/social-media/i-

will-not-be-silenced-women-targeted-hack-leak-attacks-n1275540 is annexed herewith and marked as **Annexure P-26 [Pages 294 to 303].**

Government of India's response to present allegations

59. The Government of India, in response, has not yet categorically stated that it did not and does not use Pegasus spyware. An unsigned and undated response was initially made available by ANI on 18.07.2021, ostensibly in response to queries by the Washington Post, and stated that "there has been no unauthorised interception by Government agencies". Shri Ashwini Vaishnaw, the present Union Minister of Electronics & Information Technology stated the same in the Parliament on 18.07.2021.

A copy of the unsigned Government of India's response published by ANI at the url < https://twitter.com/ANI/status/1416800154871468036> is annexed herewith and marked as **Annexure P- 27 [Page 304 – 305]**

A copy of present Union Minister of Electronics & Information Technology, Shri Ashwini Vaishnaw's statement in Parliament on "Alleged use of spyware Pegasus to compromise phone data of some persons as reported in Media on 18th July 2021" is annexed herewith and marked as **Annexure P- 28 [Page 306 to 307].**

60. The Pegasus cyber-attacks, *prima facie*, disclose the commission of several serious offences under the IT Act, 2000; the Indian Penal Code, 1860; the Indian Telegraph Act, 1885; and the Official Secrets Act, 1923. Further, the Pegasus

cyber-attacks constitute a gross violation of the fundamental rights to privacy. The use of Pegasus and other spyware, hacking and electronic surveillance against journalists severely infringes freedom of the press. This has a chilling effect on free speech and erodes democratic accountability. Most crucially, the use of spyware by the Executive government against Indian citizens would amount to serious abuse of power, which would offend the essence of constitutional democracy.

61. The citizens of India have a right to know if the Executive government is infringing the limits of their authority and what steps have been taken to safeguard their fundamental rights. The Petitioners are before this Hon'ble Court to seek the enforcement of this right, in performance of their obligations as trustees of the public, and on behalf of all citizens of India. Journalists are tasked with enforcing the public's right to be informed, to accountability, and to open and transparent government. The Petitioner's members and all journalists have duty in our democracy of holding all branches of government accountable by seeking information, explanations and constitutionally valid justifications for state action and inaction.

62. Fulfilling this responsibility requires freedom of the press which in turn relies on non-interference by the government and its agencies in reporting of journalists, including their ability to securely and confidentially speaking with sources, investigate abuse of power and corruption, expose

governmental incompetence, and speak with those in opposition to the government.

63. It is regretfully submitted that all attempts to seek accountability and enforce constitutional limits through Parliamentary processes have been stonewalled. Through their intransigence, the Respondents have deliberately avoided public debate on this issue and have provided obfuscated answers, forcing the Petitioner to approach this Hon'ble Court. The Petitioners also seek a court appointed Special Investigation Team monitored by this Hon'ble Court to investigate every aspect of the use of Pegasus by the Government of India and against Indian citizens.

64. Finally, the Petitioner have challenged the constitutional vires of electronic surveillance, hacking and use of spyware, and of the existing legal architecture for surveillance, in light of the gigantic leaps in technology and surveillance capabilities. The indiscriminate use of these capabilities against journalists and other democratic actors destroys freedom of speech and poisons the heart of democratic accountability. The Petitioners, are therefore, constrained to seek the intervention of this Hon'ble Court in enforcing Rule of Law, public accountability, ensuring law and order, and safeguarding of fundamental rights, including freedom of speech and expression and privacy.

65. In light of the aforesaid facts, the following **QUESTIONS OF LAW** have arisen:

A. Whether citizens of India are entitled to a fair and impartial investigation by a Supreme Court appointed

Special Investigation Team to uncover and be informed of the perpetrators, scale and nature of the cyber-attacks perpetrated against Indian citizens through the use of spyware/hacking/electronic surveillance tools, including such tools manufactured and/or licensed by 'NSO Group' or its group companies and/or affiliates?

B. Whether citizens of India are entitled to a fair and impartial investigation under the continuous monitoring of this Hon'ble Court?

C. Whether the right to freedom of speech and expression under Article 19(1)(a) of the Constitution of India has been violated by use of spyware/hacking/electronic surveillance against Indian citizens?

D. Whether the use of spyware/hacking/electronic surveillance tools against journalists has a chilling effect on freedom of speech under Article 19(1)(a) of the Constitution of India?

E. Whether the use of spyware/hacking/electronic surveillance tools against journalists constitutes a violation of freedom of the press protected under Article 19(1)(a) of the Constitution of India?

F. Whether the right to privacy has been violated by use of spyware/hacking/electronic surveillance tools against Indian citizens or its use in India?

G. Whether the use of spyware/hacking/electronic surveillance tools against journalists constitutes a violation of democracy which is a Basic Feature of the Constitution of India?

H. Whether the right to know of Indian citizens is violated by failure to disclose full information about the perpetrators, scale and nature of the cyber-attacks perpetrated against Indian citizens through use of spyware/hacking/electronic surveillance tools manufactured and/or licensed by 'NSO Group' or its group companies and/or affiliates?

I. Whether the right to know of Indian citizens is violated by failure to disclose whether the Government of India has a past or subsisting contract/agreement/memorandum, by whatever name it may be called, with the 'NSO Group' or its group companies and/or affiliates for use/licensing/purchase of their spyware, hacking, and other electronic surveillance products, including the spyware popularly referenced as 'Pegasus'?

J. Whether the right to know of Indian citizens is violated by failure to disclose whether the Government of India has authorised the use of spyware, hacking, and other surveillance tools licensed/purchased/obtained from the 'NSO Group' or its group companies and/or affiliates, including the spyware popularly referenced as 'Pegasus'?

K. Whether the right to know of Indian citizens is violated by failure to disclose whether the Government of India has authorised the use of spyware, hacking, or other electronic surveillance tools for interception, monitoring or decryption under Section 69 of the Information

Technology Act, 2000 and rules framed thereunder or any other existing law?

L. Whether the right to know of Indian citizens is violated by failure to disclose whether the Government of India has authorised the use of spyware, hacking, or other electronic surveillance tools for interception, monitoring or decryption under Section 5(2) of the Indian Telegraph Act, 1885 and rules framed thereunder or any other existing law?

M. Whether the right to know of Indian citizens is violated by failure to disclose the Government of India's subsisting policies, standard operating procedures, guidelines, circulars or other standards on the use of spyware, hacking, or other electronic surveillance tools against Indian citizens?

N. Whether the use of spyware/hacking/electronic surveillance against Indian citizens violates India's Binding Obligations under the International Covenant for Civil and Political Rights, the Universal Declaration of Human Rights, and customary international law?

O. Whether there has been violation of Separation of Powers by the use of spyware/hacking/electronic surveillance against persons holding constitutional office?

P. Whether there has been violation of Judicial Independence by the use of spyware/hacking/electronic surveillance against persons holding constitutional office?

Q. Whether the use of spyware/hacking/electronic surveillance exceeds lawful authorisation under Section 5(2) of the Indian Telegraph Act, 1885 and rules framed thereunder?

R. Whether the use of spyware/hacking/electronic surveillance exceeds lawful authorisation under Section 69 of Information Technology Act, 2000 and rules framed thereunder?

S. Whether Section 5(2) of the Indian Telegraph Act, 1885 violates Article 19(1)(a) of the Constitution of India?

T. Whether Section 5(2) of the Indian Telegraph Act, 1885 violates the right to privacy?

U. Whether Section 5(2) of the Indian Telegraph Act, 1885 and rules framed thereunder violates Article 19(1)(a) of the Constitution of India?

V. Whether Section 5(2) of the Indian Telegraph Act, 1885 and rules framed thereunder violates the right to privacy?

W. Whether Section 69 of Information Technology Act, 2000 and rules framed thereunder violates Article 19(1)(a) of the Constitution of India?

X. Whether Section 69 of Information Technology Act, 2000 and rules framed thereunder violates the right to privacy?

Y. Whether Indian citizens are entitled to a recourse and remedy in the event that their fundamental right to privacy is found to be violated by use of spyware, hacking and/or electronic surveillance against them?

66. Therefore, the issuance of a writ, direction or order of any description is being sought on the following **GROUNDS**:

CITIZENS HAVE A RIGHT TO KNOW

A. BECAUSE, it is respectfully submitted that citizens of India have a right to know about the violation of fundamental rights, abuse of power by the state, occurrence of cyber terrorist attacks, and threats to their privacy, safety and freedoms.

B. BECAUSE, the 'right to know' or the 'right to information' of citizens is a fundamental right protected by Article 19(1)(a) and Article 21 of the Indian Constitution. This right is essential to the full exercise of other civil and political rights, including the right to privacy as autonomy, right to equality, right to freedom of speech and expression, and the right to full participation in democratic processes.

C. BECAUSE, the Government of India has not expressly denied procuring Pegasus spyware, or using it on journalists, and consequently must uncover and furnish all information regarding purchase and use of this malware, and illegal surveillance carried out by the use of this spyware/surveillance tool/hacking.

Citizens have a Right to Know about Abuse of Power

D. BECAUSE the use of spyware, hacking and electronic surveillance on Indian citizens by the state would amount to gross abuse of power.

E. BECAUSE the Indian Constitution instituted a republican form of government, where power lies not in

the hands of any public official but inheres in each citizen. Each public official exercises powers only under the limited authority granted by the Constitution of India. Each branch of government is constrained by the Constitution and is accountable to the public, as agents of their sovereign power.

F. BECAUSE the Pegasus cyber-attacks point to a severe inversion of this power structure. The possible use of military weapons against citizens is a serious abuse of power and a gross perversion of the constitutional scheme of limited government. Citizens are entitled to know if the Executive government is infringing the limits of their authority and what steps have been taken to safeguard their fundamental rights.

G. BECAUSE, this Hon'ble Court recognised the importance of the right to know for public accountability in the 7 judge bench decision in ***State of U.P v. Raj Narain*** reported in AIR 1975 SC 865. This Hon'ble Court, speaking through Hon'ble Mr. Justice K. K. Mathews, observed as follows:

"In a government of responsibility like ours, where all the agents of the public must be responsible for their conduct, there can be but few secrets. The people of this country have a right to know every public act, everything that is done in a public way, by their public functionaries. They are entitled to know the particulars of every public transaction in all its bearing… To cover with veil of secrecy the common routine business is not

in the interest of the public. Such secrecy can seldom be legitimately desired. It is generally desired for the purpose of parties and politics or personal self-interest or bureaucratic routine. ***The responsibility of officials to explain or to justify their acts is the chief safeguard against oppression and corruption****."*

[emphasis added]

Citizens have a right to know about public safety and violations of their fundamental rights

H. BECAUSE the use of military grade cyber weapons against Indian citizens is a grave breach of individual fundamental rights and threat to public safety. The use of military grade spyware on public actors, including members of intelligence agencies, holders of constitutional office, and political leaders, is a severe threat to national security. It is imperative that the public is made aware as who is responsible for the use of these cyber weapons: whether it be the Indian government, foreign powers, private corporations, or unscrupulous persons. The Petitioners are duty bound to ensure that the public is informed about the perpetrators, scale and impact of these criminal actions and breaches of fundamental rights, and measures taken to prevent such further occurrences.

I. BECAUSE citizens of India have a right to know about violations of their fundamental rights. This is not merely a matter of personal safety and dignity, but also so that individuals can avail of constitutional remedies for such

violations. This includes petitioning this Hon'ble Court for the issuance of writs to stop all such violations, seeking compensation for commission of constitutional torts, seeking statutory damages for infringement of privacy under Section 43 of the Information Technology Act, 2000, and to seek directions against the Respondents to take necessary measures to protect them from any future violations.

Citizens have a right to know to ensure full participation in the democratic process

J. BECAUSE civic republicanism places full participation of the citizen at the centre of the democratic process. The citizen must be informed of all policies and actions by the state, to ensure one's full participation in democratic processes and institutions.

K. BECAUSE the exercise of the right to freedom of speech and expression, including the right to full participation in democratic processes requires that all information necessary for public deliberation is available to the public. Deliberative democracy is stilted without the government of the day disclosing its policies and actions, and justifications for the same.

L. BECAUSE journalists their role as agents of public reason through public debate and deliberation without full information about the government's actions and policies.

M. BECAUSE information about the government's policies is necessary for informed choices by voters in the

electoral process. The right to exercise one's franchise has no meaning if citizens are not informed about the actions and policies of an incumbent, so as to make an informed choices about whether these policies ought to be continued or not.

Citizens have a right to know about the integrity of democratic processes

N. BECAUSE the Pegasus cyber attacks have raised severe questions as to the integrity of several democratic institutions and the political process. Amongst names on the list of potential targets is included a former Election Commissioner, several members of the Opposition, and political strategists. If unaddressed, this can shake the public faith in democratic processes, and create a chilling effect, which is poisonous to the health of any democracy.

O. BECAUSE the participation of individuals in democratic processes hinges on its fairness and integrity. If citizens are left to believe that one's chances of successfully engaging in the democratic process are doomed from the start due to indiscriminate illegal surveillance by persons in power, including against political rivals, this will have a strong deterrent effect on public participation in democratic processes and institutions. If politicians and elected legislators are under fear of illegal surveillance, this will severely impact their ability to exercise their responsibilities as public actors, which must include exposing, critiquing

and opposing state action. The failure to disclose the scale and nature of illegal surveillance will halt the free exchange of ideas and the free flow of information. This can render a death blow to democracy, which must be urgently protected from such corrosion.

Snooping on journalists violates the public's right to know

P. BECAUSE democracy requires and implies informed citizens. Journalists, as the fourth estate, fulfil the role of informing the public, and have the responsibility of holding all branches of government accountable for their actions through informing public deliberation. The role of the press in informing the public was observed per the majority opinion speaking through Hon'ble A. N. RAY. J. (as he was then) in ***Bennett Coleman (supra):***

> "**80**. The faith of a citizen is that political wisdom and virtue will sustain themselves in the free market of ideas so long as the channels of communication are left open. The faith in the popular Government rests on the old dictum, "let the people have the truth and the freedom to discuss it and all will go well." The liberty of the press remains an "Art of the Covenant" in every democracy."

Hon'ble MATHEW J., though speaking in dissent, upheld this principle, observing:

> **"167.** The matter can be looked at from another angle. The constitutional guarantee of the freedom of speech is not so much for the benefit of the press as it is for the benefit of the public. The freedom of speech includes within its compass the right of all citizens to read and be informed. In *Time* v. *Hill* [385 US 374] the U.S. Supreme Court said:
>
> "The constitutional guarantee of freedom of speech and press are not for the benefit of the press so much as for the benefit of all the people."
>
> **168.** In *Griswold* v. *Connecticut*, [381 US 479, 482] the U.S. Supreme Court was of the opinion that the right of freedom of

> speech and press includes not only the right to utter or to print, but the right to read.
>
> **169.** As I said, the freedom of speech protects two kinds of interest. There is an individual interest, the need of men to express their opinion on matters vital to them and a social interest in the attainment of truth so that the country may not only accept the wisest course but carry it out in the wisest way. "Now, in the method of political Government, the point of ultimate interest is not the words of the speakers, but the minds of hearers .... The welfare of the community requires that those who decide issues shall understand them." [Meiklejohn, Political Freedom, p. 26] "The general principles underlying first amendment safeguards may, for present purposes, be reduced to three judicially recognized specifics. First, Professor Alexander Meiklejohn's assertion that the first amendment was intended to define not an individual right to speak, but rather, a community right to hear has been assumed by modern constitutional decision (*Rosenblatt* v. *Baer* [383 US 75, 94, 95 (1966)] *Lamont* v. *Postmaster General* [381 US 301] , *Roth* v. *United States* [354 US 476, 484] , *Stromberg* v. *California*, [283 US 359, 369] (see Paul Goddstein, *Copyright and the First Amendment*) [Columbia Law Review, Vol. 70, 983, 989] . That the right of the public to hear is within the concept of the freedom of speech is also clear from the pioneering opinion of Justice Burger, as he then was, in *Office of Communication of United Church of Christ* v. *F.C.C.* [Federal Reporter, 359, 2nd series, 994] The learned Judge emphasised principally the primary status of "the right of the public to be informed, rather than any right of the Government, any broadcasting licensee or any individual member of the public to broadcast his own particular views on any matter"."

Q. BECAUSE this Hon'ble Court in ***Indian Express Newspapers (Bombay) (P) Ltd. (supra)*** quoted with appreciation the above observations of Hon'ble MATHEW J. (writing in dissent) and held that "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."

R. BECAUSE in ***Printers (Mysore) Ltd. v. CTO (supra),*** this Hon'ble Court speaking through Hon'ble JEEVAN

REDDY J. held that freedom of the press would mean informing the public about the misdeeds of the government:

> "13..The newspapers not only purvey news but also ideas, opinions and ideologies besides much else. They are supposed to guard public interest by bringing to fore the misdeeds, failings and lapses of the Government and other bodies exercising governing power. Rightly, therefore, it has been described as the Fourth Estate."

S. BECAUSE, infringements on freedom of the press through surveillance of journalists severely curtails their ability to freely uncover, expose, provide information about public action. This neutralising of journalists' roles violates the right to know of all citizens and dangerously tilts the balance of power in favour of the political class and away from the people.

ELECTRONIC SURVEILLANCE AND HACKING VIOLATES FREE SPEECH UNDER ARTICLE 19(1)(a)

T. BECAUSE, spying, electronic surveillance and hacking violates the right to freedom of speech, and, the right to a freedom of the under Article 19(1)(a), by causing a chilling effect on the exercise of free speech particularly by journalists and their possible sources.

U. BECAUSE this Hon'ble Court has held in ***Shreya Singhal v. Union of India***, reported in (2013) 12 SCC 73 that any state action that is "liable .. to be used in such a way as to have a chilling effect on free speech and would, therefore, have to be struck down." The use of electronic surveillance and spyware, especially in the nature of Pegasus, on journalists has a strong chilling effect on the freedom of the press. The use of spyware

which has cataclysmic surveillance capabilities including activating cameras on personal devices, recording audio of confidential conversations, accessing private images, communications, GPS location and so on renders any confidential communication with whistle blowers and other sources impossible. This curtails the ability of journalists to uncover facts, and especially to undertake investigative reporting aimed at public accountability.

V. BECAUSE diminishing the freedom of the press curtails the free flow of ideas and damages deliberative democracy. This Hon'ble Court in ***Sakal Papers P. Ltd. v. Union of India*** reported in 1962 AIR 305 has affirmed the centrality of freedom of the press "under a democratic Constitution which envisages changes in the composition of legislatures and governments," and emphasised that any regulation that would necessarily "undermine… power to influence public opinion" was "capable of being used against democracy as well."

W. BECAUSE surveillance has a chilling effect on the free speech of all citizens, which erodes democracy. This Hon'ble Court in ***S. Rangarajan v. P. Jagjivan Ram & Ors***. reported in 1989 (2) SCC 574 observed the critical role of freedom of speech and public deliberation for the working of democracy:

> "36. The democracy is a Government by the people via open discussion. The democratic form of Government itself demands its citizens an active and intelligent participation in the affairs of the community. The public discussion with people's participation is a basic feature and a rational process of democracy which distinguishes it from all other forms of

Government. The democracy can neither work nor prosper unless people go out to share their views."

THERE HAS BEEN GROSS VIOLATION OF THE RIGHT TO PRIVACY UNDER THE CONSTITUTION

The right to privacy is a fundamental right, which can only be restrained when it passes proportionality review

X. BECAUSE the right to privacy is a fundamental right under the Constitution of India. In ***K. S. Puttwaswamy (supra)***, a nine-judge bench of this Hon'ble Court affirmed the right to privacy as a fundamental right and provided a four step framework for testing any state action under the right to privacy: (1) legality, (2) legitimate aim, (3) proportionality and (4) procedural safeguards. In this regard, Hon'ble Chandrachud J. speaking for the plurality noted that:

*"***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."

Hon'ble Sanjay Kishan Kaul J. similarly identified the test as follows:

*"**71**. The concerns expressed on behalf of the petitioners arising from the possibility of the State infringing the right to privacy can be met by the test suggested for limiting the discretion of the State:*

(i) The action must be sanctioned by law;

(ii) The proposed action must be necessary in a democratic society for a legitimate aim;

(iii) The extent of such interference must be proportionate to the need for such interference;

(iv) There must be procedural guarantees against abuse of such interference."

Y. BECAUSE, this four-part test has been evolved in the context of the rich jurisprudence constraining state action under Articles 14, 19 and 21. Under this jurisprudence, state action must be just, fair and reasonable. Any restrictions to the exercise of fundamental rights are exceptional and must closely follow the grounds for reasonable restrictions stated in Article 19.

Z. BECAUSE a Constitution Bench of this Hon'ble Court in ***K. S. Puttaswamy v. Union of India II, Aadhaar (supra)***, further clarified the standard of proportionality review to be used in considering the legality of action that infringes the right to privacy as follows:

"267. The concept and contours of doctrine of proportionality have already been discussed in detail.

We have also indicated the approach that we need to adopt while examining the issue of proportionality. This discussion bring out that following four subcomponents of proportionality need to be satisfied: (a) A measure restricting a right must have a legitimate goal (legitimate goal stage). (b) It must be a suitable means of furthering this goal (suitability or rationale connection stage). (c) There must not be any less restrictive but equally effective alternative (necessity stage). (d) The measure must not have a disproportionate impact on the right holder (balancing stage).”

Use of Pegasus violates the *Puttaswamy* tests

AA. BECAUSE the Pegasus spyware grossly fails on all four limbs of the ***Puttaswamy*** (supra) tests. There is no ostensible legal authority for hacking and use of military grade extensive and invasive electronic surveillance against Indian citizens. Citizens have a right to know the legal authority behind the use of such weaponry by the state.

BB. BECAUSE the use of surveillance against journalists, political rivals, holders of constitutional office and other citizens attacks the very essence of democratic integrity and accountability and can never be a legitimate state aim.

CC. BECAUSE hacking and electronic surveillance through spyware cannot be a suitable means for furthering any legitimate goal of the state in public safety or national

security. The careful balance between coercive power of the state and the essence of limited government was reflected in the choice to assign and withhold specific powers to the police under the Code of Criminal Procedure, 1973. The means for coercive action are captured in the power to arrest and the powers of search and seizure permitted under the said Code. These extraordinary powers are triggered when the police obtain jurisdiction to investigation into the occurrence of a criminal offence. The power of search and seizure are not broad sweeping powers that can be exercised at will in the expectation of the occurrence of possible criminal action, or as a means to target journalists and political opponents. Similarly, Section 69 of the IT Act, 2000 does not and cannot authorise hacking of electronic devices or its contamination by malware.

DD. BECAUSE the Pegasus spyware, by its very design, can never pass the tests of necessity and proportionality. The use of Pegasus infects a user's electronic device in a way that allows the attacker to take complete control over the device. This act of hacking cannot be ever considered either necessary or proportionate. The breadth of the invasive hacking powers of the Pegasus spyware militates against any notion of proportionality. In any event, the complete opaqueness with the use of Pegasus prevents any analysis on necessity.

EE. BECAUSE the content of fundamental rights must inform governmental policy from its very inception.

These rights form the architecture for governance in our country and must be present at the very initial stage in the design of technological interventions. The design of military grade spyware is not done within any framework of constitutional rights or safeguards, or even international human rights law. Privacy cannot be a plug in or update that is added onto a technological weapon after its rollout. The domestic use of the Pegasus spyware, which by its very design is meant for extra constitutional action, has no place in our constitutional scheme.

FF. BECAUSE no ostensible procedural safeguard have been put in place for use of cyber-arms, spyware, hacking, spying and electronic surveillance against citizens. Citizens have a right to know about all steps, if any, that have been taken to remedy this gross infringement of rights.

Right to privacy is protected under international human rights law

GG. BECAUSE international human rights law not only recognises the right to privacy, but also imposes higher burdens on governments for actions that infringe privacy. Under international law, any collection and processing of data, even under a public emergency or public safety interest, must meet the tests of legality, legitimate aim, necessity and proportionality. [United Nations Human Rights Council, "Resolution adopted by the Human Rights Council on 23 March 2017: The Right

to Privacy in the Digital Age," UN Doc No. A/HRC/RES/34/7 (April 7, 2017); Necessary and Proportionate: International Principles on the Application of Human Rights to Communications Surveillance, (May 2014), available at https://necessaryandproportionate.org/files/2016/03/04/en_principles_2014.pdf].

HH. BECAUSE the principles of necessity and proportionality, adopted by this Hon'ble Court in ***Puttaswamy (supra)***, have been crystallised into the Fair Informational Practice Principles (FIPP), the OECD Privacy Framework, 2013 (OECD Framework) and the General Data Protection Regime (GDPR) which have identified the following principles for safeguarding privacy when any data is accessed or collected. These principles have also been adopted in the Personal Data Protection Bill, 2019, indicating the broad acceptance of these standards at the normative level to the Indian context.

- The data minimisation principle: which requires that data collected and processed should not be held or further used unless this is essential for reasons that were clearly stated in advance.
- The purpose specification principle: which requires a clear purpose set out prior to the initiation of data collection.

• The use limitation principle: which requires that the data be utilised for the use specified prior to the collection and not be expanded to other uses.

• The openness principle: which foregrounds transparency in design, storage, sharing and use of data.

• The security safeguards principle: which requires robust data security infrastructure and practices.

• The individual rights and participation principle: which requires democratic consultation and participation in evolving of new policies.

• The accountability principle: which means setting in place a remedy for misuse of data.

• Sunset clause: which requires and end goal and end date for the project

II. BECAUSE Pegasus spyware, marketed as military grade malware, is deliberately designed to operate outside any of the above principles. The use of Pegasus on citizens is a clear violation of international human rights law.

JJ. BECAUSE spying, hacking and electronic surveillance grossly exceeds the limits of necessity and proportionality as articulated in the above principles.

<u>The Union of India has failed to protect the right to privacy</u>

KK. BECAUSE the Union of India has failed to act to safeguard the fundamental right to privacy of all persons in India and all Indian citizens. The detection of Pegasus spyware on at least 10 devices of Indian citizens by forensic experts reveals the commission of serious

infringements to privacy and violations of law. The Union of India is responsible to ensure that such violation do not occur and have failed to do so.

EXCEEDS ANY POSSIBLE LAWFUL AUTHORISATION

LL. BECAUSE using spyware and hacking by the state, including use of Pegasus, goes several steps beyond the statutory framework for surveillance in India. The indiscriminate targeting of citizens is not contemplated by the law which has been put in place by the legislature i.e., Section 69 of the IT Act, 2000 and more particularly the IT Interception Rules, 2009. The procedural framework provided therein does not allow for **hacking** of mobile phone devices and contamination of phones by remote **installation of malware** such as Pegasus.

MM. BECAUSE the existing framework under Section 5(2) of the Indian Telegraph Act, 1885 and under Section 69 of the IT Act, 2000 merely applies the minimum standards laid down in ***PUCL v. Union of India (supra)*** for interception of telecommunication devices. These were not designed to authorise hacking of devices, especially when considered in the context of the cataclysmic leaps in cyber weaponry since then. These existing procedures for interception, if extended to include hacking, would severely fall short of any meaningful protection to privacy.

NN. BECAUSE in the absence of a legislative scheme for electronic surveillance, hacking and spying, this Hon'ble

Court may be pleased to frame guidelines to ensure that the fundamental rights of all Indian citizens and all persons residing in India are safeguarded from infringement by use of these tools.

EXISTING LAW IS ULTRA VIRES THE CONSTITUTION

OO. BECAUSE, in any event, the existing legal architecture for interception and monitoring of communications is *ultra vires* the Constitution of India. The present legal provisions do not meet the standards of proportionality review laid down by this Hon'ble Court in ***Puttaswamy (supra)***, and ***K.S. Puttaswamy v Union of India (II)(Aadhaar) (supra).***

PP. BECAUSE both regimes under Section 5(2) of the Indian Telegraph Act, 1885 along with rules framed thereunder and Section 69 of the Information Technology Act, 2000 along with rules framed thereunder do not apply the standards of necessity while authorising interception and monitoring.

QQ. BECAUSE both regimes under Section 5(2) of the Indian Telegraph Act, 1885 along with rules framed thereunder and Section 69 of the Information Technology Act, 2000 along with rules framed thereunder do not the require that interception and monitoring, when authorised, is extremely narrowly framed to ensure that it is targeted at the least possible collecting of information that strictly meets the standard

of necessity while authorising interception and monitoring and therefore is disproportionate.

RR. BECAUE in the absence of parliamentary or judicial oversight, electronic surveillance gives the executive government the power to influence the subject of surveillance as well as all classes of persons.

SS. BECAUSE both regimes under Section 5(2) of the Indian Telegraph Act, 1885 along with rules framed thereunder and Section 69 of the Information Technology Act, 2000 and rules framed thereunder grant unchecked power to the executive government. These provisions are agnostic with respect to the subject of surveillance, and surveillance takes place without any checks outside the executive wing of government. This means that there are no checks in place to ensure that democratic actors like journalists are not made the target of surveillance.

TT. BECAUSE the guidelines laid down in ***PUCL v. Union of India (supra)*** were framed in the context of the limited capabilities for phone tapping in 1996 and have now been rendered obsolete. Technological advances since then allowed exponential expansion in surveillance capabilities. Individual phones store unprecedented treasure troves of personal information. This includes intimate correspondence, emails, photographs, banking, health information, bodily activity records (including second by second cataloguing of heart rate, menstrual logs, etc.), biometrics, GPS location, internet search

history, shopping history and so on. This expansion in the quality and quantity of intimate and sensitive personal information on our phones and other electronic devices necessitates the evolving of new standards for access to these devices. Prior judicial orders by issuing a warrant for search or seizure pursuant to an investigation would be a precondition for the state to access many categories of such information. Therefore, these guidelines are rendered obsolete and this Hon'ble Court may be pleased to frame new guidelines that are in consonance with present and future developments in technology.

UU. BECAUSE both regimes under Section 5(2) of the Indian Telegraph Act, 1885 along with rules framed thereunder and Section 69 of the Information Technology Act, 2000 along with rules framed thereunder do not meet the necessary standards for freedom of the press and freedom of speech and expression.

ELECTRONIC SURVEILLANCE/ HACKING VIOLATES CONSTITUTIONAL BALANCE OF POWER

VV. BECAUSE, electronic surveillance, hacking and spying by the Executive is an unlawful infringement on the autonomy of the Legislative and Judicial branches and would violate separation of power between the executive, legislature and judiciary.

WW. BECAUSE electronic surveillance, hacking and spying on judges is a gross violation of judicial independence which is a Basic Feature of the Constitution of India.

XX. BEAUSE fear of electronic surveillance legislators in Parliament of India and various legislatures in the States across India interferes with their ability to exercise their constitutional role as a check to Executive power.

YY. BECAUSE electronic surveillance, hacking and spying on journalists infringes on the independence of the Fourth Estate, which serves as an independent means of checks and balances on all branches of government. Hacking of the phones of journalists violates their Part III rights, undermines democracy, deprives the citizens of India of meaningful public deliberation, and threatens the entire process of democratic accountability.

THERE HAS BEEN COMMISSION OF SEVERAL COGNIZABLE OFFENCES AGAINST INDIAN CITIZENS AND IN INDIA

ZZ. BECAUSE targeted hacking using Pegasus spyware violates Section 43(a), (b), (c) and (d) of the Information Technology Act, 2000 by accessing the smartphone, introducing a ‘contaminant’ or ‘virus’, damaging the smartphone and extracting data from it without the permission of the owner of the smartphone. According to the definitions provided in Section 43 of the IT Act, 2000 Pegasus can be defined under the Act as a ‘computer virus’ and a ‘computer contaminant’ since it

is designed to attach itself to a targeted device, and then modify, record and transmit data from the targeted devices. Violations of S.43 of the IT Act, 2000 are liable for civil damages and also punishable under Section 66 of Act with imprisonment upto three years and/or fine. Further, Section 66B of the IT Act, 2000 punishes the dishonest receiving of stolen computer resources (Section 2(k) includes 'data' in the definition of 'computer resource'). There is also the *prima facie* commission of an offence under Section 72 of the IT Act, 2000, for breach of privacy and confidentiality.

AAA. BECAUSE, the use of the camera hacking feature through spyware, including Pegasus, against women who work as journalists also attracts Section 66E of the IT Act, 2000 which prohibits capturing, publishing and transmitting of images of a private area of any person which is punishable with imprisonment for three years or with fine.

BBB. BECAUSE the use of Pegasus spyware attracts the offence of cyber-terrorism as defined under Section 66F of the IT Act, 2000 which is punishable with imprisonment which may extend to imprisonment for life.

CCC. BECAUSE the use of Pegasus spyware against public officials constitutes offences under Sections 3 and 15 of the Official Secrets Act, 1923.

DDD. BECAUSE the use of spyware by foreign governments against Indian citizens, and important

public decision makers, in particular, is a severe threat to public safety at the very least, and potential threat to national security. This requires urgent investigation by the most competence and impartial investigators under monitoring of this Hon'ble Court.

THE USE OF PEGASUS VIOLATES FREEDOM OF PROFESSION UNDER ARTICLE 19(1)(g)

EEE. BECAUSE surveillance, whether using Pegasus or under Section 69 of the IT Act, 2000 violates the right to freedom of speech, the right to freedom of profession of journalists who are precluded from undertaking safe investigative reporting.

FFF. BECAUSE surveillance impedes the free flow of ideas and information, and has a chilling effect on public actors holding the government accountable. This has a severely detrimental impact on the ability of politicians and public officials to freely exercise their freedom of profession.

GGG. The Petitioners crave liberty to raise additional grounds during the course of arguments.

36. The Petitioners have filed this Petition seeking issuance of a Writ of Mandamus or any other appropriate writ, direction or order for disclosure of information as to the violation of fundamental rights, abuse of power, and commission of criminal offences through use of electronic surveillance, hacking and spyware against Indian citizens, and, fair and impartial investigation by a special investigation team appointed and monitored by this Hon'ble Court since the

Petitioners have no alternate efficacious remedy but to approach this Hon'ble Court under Article 32 of the Constitution of India for the reliefs prayed for herein.

37. That the Petitioners have not filed any other Petition before this Hon'ble Court or before any other Court seeking the same relief.

38. That this Hon'ble Court has the jurisdiction to entertain and try this Petition.

39. That it is humbly submitted the present issue is a fit case to be entertained as a public interest litigation.

40. That the Petitioners crave leave to alter, amend or add to this Petition.

41. That the Petitioners seek leave to rely on documents, a list of which, along with true typed copies has been annexed to this Petition.

42. That this Petition has been made *bona fide* and in the interest of justice.

PRAYER

In the above premises, it is prayed that this Hon'ble Court may be pleased to:

(i) Issue a writ of mandamus to the Union of India to produce the orders issued authorising the interception, monitoring and decryption of electronic communication devices of Indian citizens under the relevant law and rules, with the reasons in writing for issuance of the same, as mandated by law; and/or,

(ii) Issue a writ of mandamus or of any other nature to the Union of India directing it to furnish information on the interception, monitoring and decryption of information by using spyware,

hacking and/or electronic surveillance in India between 2017 to the present day in 2021, including the following:

a. Did the Union of India, or any of its agencies, procure, license, obtain and/or use the spyware 'Pegasus' from 'NSO Group' or its group companies and/or affiliates on Indian Citizens?
b. Did the Union of India, or any of its agencies, procure, license, obtain and/or use of spyware, hacking or electronic surveillance tools of any name from 'NSO Group' or its group companies and/or affiliates on Indian Citizens?
c. Direct the Union of India to produce any contracts, agreements, memoranda of understanding entered into with foreign companies for supplying spyware, hacking or electronic surveillance for use on Indian Citizens.
d. Direct the Union of India to produce any contracts, agreements, memoranda of understanding entered into with foreign companies for supplying spyware, hacking or electronic surveillance which has been used, whether authorised or not, on Indian Citizens.
e. Direct the Union of India to disclose the details of how these spywares, hacking or electronic surveillance tools were paid for.
f. Direct the Union of India to disclose the details of the list of people that have been under electronic surveillance, hacking, or otherwise spied on, including the details of who prepared and populated

the said list and the details of every Indian citizen on the list.

g. Direct the Union of India to disclose the details of how many of the Indian Citizens who have been under electronic surveillance, hacking, or otherwise spied on, were charged with indulging in serious crime. and/or,

(iii) Constitute an independent special investigation team to investigate the procurement and use of spyware, hacking or electronic surveillance tools such as 'Pegasus' in India; and/or,

(iv) Issue a writ of continuing mandamus and monitor the investigation into the procurement and use of spyware, hacking or electronic surveillance tools such as 'Pegasus' in India; and/or,

(v) Issue guidelines on surveillance against Indian citizens including:

a. guidelines for the safeguarding of journalists from surveillance including electronic surveillance, spying and hacking; and

b. guidelines for the safeguarding of women who work as journalists from gendered crimes through surveillance, including electronic surveillance, spying and hacking; and/or,

(vi) Issue a writ in the nature of mandamus or any other appropriate writ, direction or order declaring Section 5 (2) of the Indian Telegraph Act, 1885 as being unconstitutional, illegal and void, and/or,

(vii) Issue a writ in the nature of mandamus or any other appropriate writ, direction or order declaring Rule 419A of the

Indian Telegraph Rules, 1951 as being unconstitutional, illegal and void, and/or,

(viii) Issue a writ in the nature of mandamus or any other appropriate writ, direction or order declaring Section 69 of the Information Technology Act, 2000 as being unconstitutional, illegal and void, and/or,

(ix) Issue a writ in the nature of mandamus or any other appropriate writ, direction or order declaring the provisions of Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption) of Information Rules, 2009 as being unconstitutional, illegal and void, and/or

(x) Pass any other orders as may be deemed fit in the facts and circumstances of this case.

AND FOR THIS ACT OF KINDNESS THE PETITIONERS AS ARE DUTY BOUND SHALL EVER PRAY.

Drawn By:
Rupali Samuel, Advocate
Raghav Tankha,
Advocate

Filed By:

(Lzafeer Ahmad B F)
ADVOCATE FOR THE PETITIONERS

Place: New Delhi
Filed On: __.08.2021