IN THE SUPREME COURT OF INDIA

CIVIL ORIGINAL JURISDICTION

WRIT PETITION (CIVIL) NO. OF 2021

(Under Article 32 of the Constitution of India)

IN THE MATTER OF:

(1) Rupesh Kumar Singh,

[redacted] ...PETITIONER NO.1

(2) Ipsa Shatakshi,

[redacted] …PETITIONER NO.2

Versus

(1) UNION OF INDIA

Ministry of Electronics and Information Technology

Through the Secretary

Electronics Niketan,

6, CGO Complex,

Lodhi Road,

New Delhi – 110 003 ...RESPONDENT NO. 1

(2) MINISTRY OF HOME AFFAIRS
Through the Home Secretary
Designated Competent Authority
North Block, New Delhi
India – 110 001 ...RESPONDENT NO. 2

(All are contesting Respondents)

WRIT PETITION OF MANDAMUS UNDER ARTICLE 32 OF THE CONSTITUTION OF INDIA

To
The Hon'ble Chief Justice of India
And His Companion Justices of the
Supreme Court of India.

The humble Petition on behalf of
of the Petitioner above named.

MOST RESPECTFULLY SHOWETH:

1. The instant Petition is filed by the Petitioners due to the violation of their right to privacy under Article 21 and their rights to freedom of speech, the free press, free access to information, and the Petitioner No.1's right to work freely as journalists under Articles 19(1)(a) and 19(1)(g) of the Constitution. Both the Petitioners are citizens of India, and are based in the state of Jharkhand. Petitioner No. 1 is an independent journalist-activist and contributes to several prominent Hindi magazines and online news portals. Petitioner No. 2 is presently married to Petitioner No.1. The

present case deals with certain disclosures arising out of the use of the Israeli malware 'Pegasus', according to which detailed surveillance activities including hacking, have been carried out with respect to data stored on the Petitioners' mobiles (smart phones), which were infected, infiltrated, and hacked by the said Pegasus malware.

I. DESCRIPTION OF PARTIES

2. The Petitioner No.1 is an Indian citizen, and an independent activist of repute, with over 7 years standing. He has been both reporting as well as participating in activism on pertinent social issues such as those of displacement, the protests of the displaced people, encounters by security forces in the state, and the massive arrests of Adivasi people framed as Maoists in the state of Jharkhand. He has been contributing to various monthly Hindi magazines and online news portals for the same, some of which include 'Media Vigil', 'Gauri Lankesh News', 'The Wire' and 'Janchowk'. The Petitioner No.1 holds Aadhaar card bearing No. 7808 1280 1224 and PAN card bearing No. BULPS9134B. A true copy of the Aadhaar card copy and PAN card of the Petitioner No.1 is annexed and marked hereto as **Annexure-P-1 (Pg. Nos. 44 to 46)**.

3. Petitioner No. 2. is a citizen of India. She is presently married to the Petitioner No. 1. Petitioner No. 2 holds Aadhaar card bearing No. 2641 0232 1925 and PAN card bearing No. DWLPS4320H. A true copy of the Aadhaar card copy and PAN card of the Petitioner No.2 is annexed and marked hereto as **Annexure-P-2 (Pg. Nos. 47 to 49)**.

4. Union of India, Respondent No. 1 herein, is represented through the Secretary to the Ministry of Electronics, Information and Technology, under the Central Government, and is the nodal agency responsible for governing and implementing the provisions of the Information Technology Act, 2000 and Rules thereunder. The Hon'ble Minister has provided various responses in Parliament in respect of the recent reports surrounding the use of the Israeli spyware, Pegasus.

5. Ministry of Home Affairs, under the Central Government, is Respondent No. 2 herein, and is represented through the Home Secretary, who is the designated 'Competent Authority' by virtue of Rule 2(d)(i) of the 2009 IT Rules and is responsible for authorising directions for electronic surveillance under Section 69(1) read with Rule 3 of the 2009 IT Rules.

II. THE STATUTORY FRAMEWORK OF ELECTRONIC SURVEILLANCE AND HACKING IN INDIA

6. Primarily, the laws relating to electronic surveillance and hacking are governed under the Information Technology Act, 2000 ["IT Act"]:

   (a) Electronic surveillance: Section 69(1) of the Act authorizes the Central and State Governments to monitor, intercept, or decrypt information contained in any 'computer resource'. A 'computer resource', as defined under Section 2(1)(k), refers to a "computer, computer system, computer network, data, computer database or

software". The interception, monitoring, or decryption of information [collectively "electronic surveillance"] is carried out pursuant to the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 ["Interception Rules"], and every order must be reviewed by a three member executive 'Review Committee' to ensure compliance with the law. It is pertinent to note that the constitutionality of the provisions of electronic surveillance under Section 69 of the IT Act and the Interception Rules are under challenge before this Hon'ble Court in *Internet Freedom Foundation v Union of India*, WP No. 44 of 2019, and this petition does not touch upon those issues or the constitutionality of electronic surveillance in any way.

(b) Prohibition on hacking: Section 43 of the IT Act prohibits, without the permission of the owner, accessing or securing access to a computer, computer system or computer network or a computer resource; or downloading, copying or extracting any data, or information from such computer system. It also prohibits the introduction of any 'computer contaminant' or 'computer virus' into any computer system; or damaging or causing to be damaged, any computer system. A violation of Section 43 of the IT Act is punishable under Section 66 of the IT Act with imprisonment for up to three years or with fine of up to five lakh rupees or with both.

The explanation to Section 43 defines a 'computer contaminant' as any set of computer instructions that are designed– (a) to modify, destroy, record, transmit data or

programme residing within a computer, computer system or computer network; or (b) by any means to usurp the normal operation of the computer, computer system, or computer network. 'Computer virus' has been defined as any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed. Both of these definitions include malware such as Pegasus that were used to infiltrate the Petitioner's phone.

(c) Prohibition on dishonestly receiving hacked data: Further, Section 66B of the IT Act prohibits dishonestly receiving or retaining any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device. A violation of Section 66B is punishable with imprisonment of either description for up to three years or with fine of up to rupees one lakh or with both.

(d) Prohibition on misuse of provisions of IT Act: Section 72 of the IT Act prohibits the abuse of powers under the IT Act, and states that if any person who, in pursuance of any of the powers conferred under the IT Act or the rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such information to any other person shall be punished with imprisonment for up to two years, or with fine of up to one lakh rupees, or with both.

III. BRIEF STATEMENT OF FACTS

7. On July 18, 2021, the Petitioners were informed about the presence of their names in a list of journalists whose phones could possibly have been spied upon, through a news report by the outlet 'The Wire'. A true copy of the article dated July 18, 2021 describing the incident and titled "Snoop List Has 40 Indian Journalists, Forensic Tests Confirm Presence of Pegasus Spyware on Some", published at the The Wire is annexed herewith as **Annexure P-3 (Pg. Nos. 50 to 66).**

8. The Petitioner No. 1 perceives that he was generally targeted for reporting about the state violence against Adivasi communities in the state of Jharkhand. His entire story was carried by various dailies and e-news portals, including one by the 'The Telegraph'. Specifically, he perceives that his reporting on the late Motilal Baskey, of Giridih district, belonging to the said community, was the reason for his and his wife's surveillance. According to the Petitioner No. 1, the said victim was a porter who assisted in ferrying passengers to a nearby tourist site, whereas the ruling Bhartiya Janta Party framed him as a Maoist-suspect, and ended his life in an encounter. A true copy of the article dated July 31, 2021 describing the incident and titled "Freelance journalist on potential snoop list to move Supreme Court", published by The Telegraph is annexed herewith as **Annexure P-4 (Pg. Nos. 67 to 69)**.

9. The Petitioners cannot be certain about whether their phones continue to be tapped. The entire incident has psychologically traumatised the Petitioners and left them

constantly wondering whether they are being surveilled through their mobile phone, laptop computer, or even in real life. Such illegal hacking has severely impeded and undermined the Petitioners' practice of their respective professions of journalism and activism, because they are constantly unsure of whether their conversations with sources and publishers are being monitored; and whether there is a threat to the life and physical safety, not just of themselves, but their family members, and those that the Petitioners regularly contact in the scope of their work. The Petitioners are deeply concerned that the hacking and infiltration of their phones through the Pegasus malware will have the effect of endangering their confidential sources and/or making vulnerable to vindictive action by third parties against whose interests they acted. The Petitioners are equally concerned that the use of this kind of cyber-weapon and illegal surveillance against journalists and human rights activists will have the effect of discouraging prospective whistleblowers in the future and will all but destroy independent investigative journalism in India. The Petitioners verily believe that use of Pegasus malware to invade their privacy and other similarly placed persons will have a grave chilling effect of freedom of speech and expression in India and poses a clear and present danger to the existence of a free press that is capable of acting as a check and balance of state powers in a democracy such as ours.

Functionality of the Pegasus Spyware

10. Pegasus is a spyware, i.e. a software designed to enter your mobile device, intercept your data, and forward it to a third-party without your knowledge or permission, which is sold by NSO Group Technologies Ltd. The NSO Group is based in Herzliya, Israel, and develops and sells mobile phone surveillance software to "*licensed government intelligence and law enforcement organizations*" around the world, as per its website. The company describes itself as a "leader" in "mobile and cellular cyber warfare," and has been operating for more than 11 years, since its founding in 2010. The NSO Group has claimed that its surveillance capability is undetectable.

11. NSO, in its "Transparency and Responsibility Report 2021", says that its "*products are designed for the sole use of thoroughly vetted and approved governmental agencies charged with maintaining public safety and security*." The report also says that NSO was founded with one key mission: "*to make the world a safer place by assisting lawful investigations by state authorities to protect the security and safety of citizens against major crimes and terrorism*". Use of Pegasus, the NSO Group says, should only be directed at legitimate criminal or terror group targets. A true copy of the NSO Group's Transparency and Responsibility Report dated 30.06.2021 is annexed herewith as **Annexure P-5 (Pg. Nos. 70 to 101)**.

12. The Pegasus spyware can be installed on a target's mobile device to mine or plant data, without their knowledge,

consent, or any action on their part. The installation of Pegasus takes place through a 'zero click process', which goes beyond the traditional spear-phishing method involving messages or links, and may be installed without any action of the target, or even on just sending the target a missed call. In other words, all that an agency or a person looking to invade the privacy of an Indian citizen by mounting a Pegasus malware attack on their phone is their phone number and a license to the Pegasus malware. There is no way to defend or prevent one's phone being invaded by the Pegasus malware if the party mounting the attack is in possession of both these things. There is also no way short of a detailed forensic analysis by a highly skilled lab for an affected citizen to even know if their phone has been infected and compromised by the Pegasus malware.

13. After infiltration and installation, the malware takes control of the target's phone (including by gaining 'root-level privileges' in an iPhone) and can then collect data; view contact lists, messages, and internet browsing history; intercept communications; remotely control peripherals such as turning on the phone's camera and microphone; use GPS functions to track a target's location and movements; and track SMSes, emails, WhatsApp chats, calendar, contacts book, photos and videos etc. This makes Pegasus one of the powerful spyware and malware available, capable of surveillance and illegally hacking a target's phone through such 'zero click exploits'. A true copy of an article dated July 30, 2021 titled "Explained: Pegasus uses 'zero-click attack' spyware; what is this method?" published in

the Indian Express is annexed herewith as **Annexure P-6 (Pg. Nos. 102 to 112).**

14. Pegasus can also harvest any data from a device — both Apple and Android — and transmit it back to the attacker, as reported by Lookout in its 2016 report titled "Technical Analysis of Pegasus Spyware". This includes phone calls, call logs, SMSs, emails, photos and videos, GPS data, user passwords, calendar, browsing history, contacts book, and WiFi/router passwords. It can also activate a mobile's peripherals, such as the microphone and camera and record calls — in the words of one of the founders of the NSO Group, it turns the phone into a "walkie talkie". The Pegasus software is also highly configurable: depending on the country of use and feature sets purchased by the user of the spyware, the surveillance capabilities include remotely accessing logs, and more, from apps including Gmail, Facebook, Skype, WhatsApp, Viber, Facetime, Calendar, Line, Mail.Ru, WeChat, Surespot, Tango, Telegram, and others. Pegasus also has a novel mechanism to install and hide itself, and obtain persistence (persistence enables the malware to stay on the device even after the operating system restarts), in the system. Once it is resident, it uses a number of ways to hide its communications and protect itself from discovery. A true copy of the Lookout Report titled "*Technical Analysis of Pegasus Spyware*" dated 25.08.2016 is annexed herewith as **Annexure P-7 (Pg. Nos. 113 to 147)**.

15. Mobile phones are tightly integrated into an individual's personal and work lives and Pegasus takes advantage of a combination of features that are available on a mobile — such as the fact that a user is always connected to a WiFi, voice communications, camera, email, messaging, GPS, passwords, and contact lists. On the basis of these features, Lookout, in its report, claimed that Pegasus is the most sophisticated privately-developed spyware, on a mobile endpoint, that it has encountered. Consequently, the Petitioners believe that not just the data on his phone, but every conversation that was audible to the microphone on his mobile device and everything that was visually visible from his phone camera has also been viewed by the entity and/or persons that infected the Petitioners' mobile devices with the Pegasus malware. As is commonplace today, the Petitioners used to (that is, till they were informed of the Pegasus attack) carry their mobile phones with themselves or keep it in arms reach practically all day and night. As a result, the entity and/or persons that infected the Petitioners' mobile devices with the Pegasus malware had access to every aspect of the Petitioners' personal and professional lives - from the most mundane to the most intimate.

16. It is submitted that the 2016 version of the spyware, detected and forensically analysed by Citizen Lab and Lookout, infected phones through the "spear-phishing" method. Using this method, the attacker could send a benign-looking Website URL (through SMS, email, social media, or any other message) to an identified target. Once the user clicks on the URL, she is directed to a domain which installs the

spyware on her device. The attack occurs silently, with no indication to the user or device administrator that anything is running or that any new processes are running. Once successfully installed, the spyware — which consists of malicious code, processes, and apps — is able to spy on the user and collect and transmit their data to the Pegasus operator. The spyware can access and exfiltrate calls, messages, log, email, from multiple applications, including, but not limited to, Facebook, Skype, WhatsApp, Viber, Facetime, Calendar, Wifi passwords, etc. In this manner, Pegasus can collect a massive amount of data about the target and transmit the same to the Pegasus Data Server at its operator's premises. This chain of transmission employs a Pegasus Anonymizing Transmission Network ("PATN"), which acts as a proxy chain to hide the identity of its operator. Additionally, even if the servers at the operator's premises are destroyed, Pegasus has the ability to find new servers and establish communication with its operator.

17. The Pegasus spyware is constantly evolving, and, therefore, the version of the Spyware detected on approximately 1400 phones in 2019, and in 50,000 phones in 2021, was more complicated and dangerous than the one identified in 2016. This is because, from 2018 onwards, Pegasus used the "zero-click" method, as found by Amnesty International Security's Lab in its report dated 18.07.2021. The zero-click method uses a remote cyber attack which does not require any interaction from the target. Simply put, a device can be attacked without needing the target to click on a malicious link. This is done by successfully exploiting vulnerabilities

in the software and hardware of the phone. Once the attacker has found a vulnerability that they can exploit, they craft special data — such as a hidden text message or image file, to inject code in the target's device. This compromises the device. Once the device is compromised, the message used to exploit, self-destructs so that it is untraceable. For example, in 2019, Pegasus infected more than 1400 phones through a simple WhatsApp missed call. The Quint's article dated 20.07.2021 provides a simple explanation of zero-click attacks, and the Pegasus spyware's evolution from 2016 to 2021. A true copy of the article dated 20.07.2021 published by The Quint is annexed herewith as **Annexure P-8 (Pg. Nos. 148 to 150).**

Revelations by Citizen-Lab from 2016-2019

18. Pegasus was first uncovered when, on 10.08.2016 and 11.08.2016, Ahmed Mansoor, a human rights defender, from the United Arab Emirates, received a text message promising "new secrets" about detainees who were tortured in UAE jails. The text message required him to click a link in order to access the information. Instead of clicking, Mansoor sent the messages to Citizen Lab — a Toronto-based research laboratory that works at the intersection of cyberspace, global security, and human rights. Citizen Lab, in its report titled "The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender", reported that they recognised the links as an attack vector, i.e., method used to penetrate the target system, connected to the Israeli NSO Group. Citizen Lab classified it as a "rare find", not used as part of a targeted

attack campaign. A true copy of the Citizen Lab's Report dated 24.08.2016 is annexed herewith as **Annexure P-9 (Pg. No. 151 to 182).**

19. In its second report, in 2018, titled "Hide and Seek: Tracking NSO Group's Pegasus Spyware to operations in 45 countries", Citizen Lab found 1091 IP addresses and 1014 domain names that were potentially attacked by Pegasus, between August 2016 — when the first Pegasus-infected device was found — and August 2018. Next, it sought to identify *where* these Pegasus systems were being used, and found suspected NSO Pegasus infections in 45 countries, including India: 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. A true copy of the Citizen Lab's Report dated 18.09.2018 is annexed herewith as **Annexure P-10 (Pg. Nos. 183 to 223)**.

20. Subsequently in 2019, approximately 1400 individuals were targeted with an NSO Group exploit of Facebook's WhatsApp platform. The exploit was disclosed by WhatsApp in May 2019. More than 100 of Pegasus' targets were journalists, activists and human rights defenders, across numerous countries including India, Bahrain, the

United Arab Emirates, and Mexico. Approximately 121 Indian journalists, lawyers, scholars, and activists were also, potentially, snooped upon. The targets were, *inter alia*, Shubhranshu Choudhary, former BBC journalist who now works in Chhattisgarh as a peace activist; Shalini Gera, a Chattisgarh-based activist and close associate of Sudha Bhardwaj — one of the accused in the Elgar Parishad-Bhima Koregaon case; Nihalsingh Rathod, Nagpur-based advocate and lawyer to Surendra Gadling, one of the accused in the Elgar Parishad-Bhima Koregaon case; Bela Bhatia who is an Adivasi rights activist; and, Saroj Giri, an Assistant Professor at the Delhi University. Globally, the attack was first reported by the Financial Times in an article dated 14.05.2019.

A true copy of the article dated 14.05.2019 published in The Financial Times is annexed herewith as **Annexure P-11 (Pg. Nos. 224 to 227)**.

In India, the Indian Express, in an article published on 30.10.2019, was the first Indian publication to break the story. A true copy of the article dated 30.10.2019 published in the Indian Express is annexed herewith as **Annexure P-12 (Pg. Nos. 228 to 237)**.

21. In September 2019, WhatsApp notified the Government of India and CERT-In about an extensive security breach: the mobile phones of 121 Indian journalists, lawyers and activists had been targeted; reportedly, Pegasus had been used to intercept and extract information and communications from the victim's mobile phones. A copy

of the news report from the Hindu titled '*Alerted the Indian Govt. of spyware attack in September, says WhatsApp"* dated 03.11.2019 is annexed herewith as **(Pg. Nos. 238 to 240)**.

22. In October 2019, WhatsApp sued the NSO Group before a US District Court in California alleging that it had "d*eveloped their malware in order to access messages and other communications after they were decrypted on target devices*" and the target of civil society activists represented an "unmistakable pattern of abuse". WhatsApp sought a permanent injunction banning NSO from using its service. In July 2020, the judge ruled that the suit against the NSO Group can proceed to the stage of discovery. A copy of WhatsApp's plaint against NSO Group and copy of reports by BBC and the Guardian on WhatsApp's lawsuit is annexed herewith as **Annexure P-14 (Pg. Nos. 241 to 376)**.

23. That on 23.10.2019, Saurav Das, a Puducherry-based RTI activist filed an RTI application. In his query, he asked Respondent No.2 whether it had purchased the Pegasus spyware. If so, on what date, and if not, whether there was a proposal to purchase it. A copy of the RTI query dated 23.10.2019 is annexed herewith as **Annexure P-15 (Pg. Nos. to 377).**

24. He received a response on 31.10.2019. The CPIO, S.K. Bhalla, claimed that "no such information is available". A true copy of the Respondent No.2's response dated

31.10.2019 is annexed herewith as **Annexure P-16 (Pg. Nos. 378 to)**.

25. On 29.11.2019, the matter was raised before the Rajya Sabha by Shri Digvijaya Singh. Shri Ravi Shankar Prasad, the then Minister of Electronics and Information Technology made an elaborate statement without categorically addressing the issue of surveillance using Pegasus. He provided an account of the communications between WhatsApp and CERT-In, from May–November 2019, regarding the use of Pegasus Spyware on Indian citizens. In response, Shri Digvijay Singh sought to know whether the Government, or any of its agencies, had bought the Pegasus software from the NSO Group. Following this, an extensive debate ensued in the Parliament.

26. During the debate, several members raised crucial questions regarding the alleged surveillance of Indian citizens using the Pegasus spyware. For instance, referring to a vulnerability note published by CERT-In on 17 May 2019, Shri Md. Nadimul Haque asked, *"The severity rating of the breach was 'high' according to the note, which has since been taken down. So, my question is this. Why did the Government fail to act on this urgent note by the team at CERT-In at that time?"*. Similarly, Shri KK Ragesh asked the government, *"What steps have you taken immediately after getting the information? And why you did not caution the WhatsApp users about this security threat and the issue of snooping?"* and "*Why were the people, who were fighting against the Government, targeted?"*. Many echoed Shri

Digvijay Singh's question "*did the Indian government or any of its agencies, in any manner whatsoever, use, buy, or authorize the use of the Pegasus spyware?*"

27. Instead of categorically confirming or denying the allegations or providing a concrete response to these questions, the Hon'ble Minister at the time spoke about the successful digital ecosystem of the country, permissible restrictions on privacy, and India's legal framework of surveillance. He told the House that the Government is required to balance the competing interests of privacy and national security and that "*whenever the Government or its agencies which are authorized – I repeat it – if they have to do so for the safety and security of India, they do so only as per the Standard Operating Procedure*." The then Hon'ble Minister Shri Ravi Shankar Prasad insisted that the Government engages in "authorized surveillance" *only*. When he was repeatedly asked whether the Government of India had negotiated a deal with the NSO Group, he replied "*Sir, I think, I have very specifically stated that the security agencies responsible for all these, follow-up of terrorist attacks, etc., follow a particular procedure. If it is in violation of that, there, we take action and we take tough action, and also impose a penalty*". No details of any violations by agencies and penalties imposed thereupon were however shared by him at the time. The Hon'ble Minister also did not state whether the use of Pegasus would fall within the ambit of Section 69 of the Information Technology Act, 2000. A true copy of the transcript of the

debate in the Rajya Sabha on 28 November 2019 has been annexed herewith as **Annexure P-17 (Pg. Nos. 379 to 403)**.

28. The same issue was raised in the Lok Sabha in December 2019. In response to a member's question pertaining to the alleged hacking of accounts of Indian activists, journalists and lawyers using the Pegasus Spyware, the Hon'ble Minister of State for Electronics and Information Technology, Shri Sanjay Dhotre, in a similar manner, asserted the Government's adherence to laws and established protocols. While acknowledging WhatsApp's disclosure of a possible breach of 121 Indian users' privacy through the Pegasus spyware, the Hon'ble Minister of State stated that:

> "*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 safeguards to ensure that no innocent citizen is harassed or his privacy breached.*"

It is submitted that despite grave concerns raised in Parliament, and by national media, the Government failed to provide an adequate response and take concrete action against the Pegasus attack. Notably, however, the Minister of State stated that based on news and information in public and media on snooping of mobile devices of Indian citizens through WhatsApp by spy software Pegasus, "*CERT-In has sought submission of relevant details and information from WhatsApp and NSO group*."

CERT-In, or the Indian Computer Emergency Response Team, is the national nodal agency statutorily designated under the IT Act to work on cyber security and respond to computer security incidents as and when they occur. There is no public record of whether the NSO Group replied to CERT-In or what the details of its response were. A true copy of the Hon'ble Minister's response dated December 11, 2019 to Unstarred Question No. 3686 before the Lok Sabha has been annexed herewith as **Annexure P-18 (Pg. Nos. 404 to 405)**.

29. That on 10.04.2020, the Internet Freedom Foundation ("IFF") filed a common representation to the Governments of Maharashtra and Chattisgarh — where most of the targets of the 2019 Pegasus attack were located. IFF recommended, *inter alia,* that the State Governments of Maharashtra and Chattisgarh should establish an investigation committee to look into the hack committed into their state. However, their request did not receive any response. A true copy of IFF's representations dated 10.04.2020 is annexed herewith as **Annexure P-19 (Pg. Nos. 406 to 409)**.

30. On 21.09.2020, the Ministry of Electronics and Information Technology, in response to a question by Lok Sabha MP D.K. Suresh, categorically denied that the government or any of its agencies have access to the data and voice messages circulated through WhatsApp. A true copy of Unstarred Question No. 1662 is annexed herewith as **Annexure P-20 (Pg. Nos. 410 to)**.

31. On 24.03.2021, in response to a question in the Lok Sabha about whether the government had found the presence of Pegasus spyware in the country and launched any investigation, the Minister of State for Electronics and Information Technology stated that "no such information was available with the government." A true copy of Unstarred Question No. 4612 along with the reply is annexed herewith as **Annexure P-21 (Pg. Nos. 4 to 11)**.

2021 revelations by the Pegasus Project involving the Petitioners

32. The present petition focuses on a targeted espionage attack carried out between 2017 and 2019 that targeted the Petitioners. The attack came to light on 18.07.2021 because of an investigative effort called 'The Pegasus Project'. The Pegasus Project is a consortium of over 80 journalists from 17 highly-reputed media bodies in 10 countries — Washington Post, The Guardian, Le Monde, Süddeutsche Zeitung, Die Zeit, among others. The Consortium also includes Indian online publication "The Wire". Technical support was provided by Amnesty International's Security Lab. On the said date, the Pegasus Project revealed the illegal surveillance and hacking activities of the malware to the public. Amnesty International's Security Lab performed in-depth forensic analysis of numerous mobile devices from human rights defenders and journalists around the world and uncovered widespread, persistent and ongoing unlawful surveillance and human rights abuses perpetrated using NSO Group's Pegasus spyware.

33. The investigation was coordinated by Paris-based journalism non-profit "Forbidden Stories". Forbidden Stories and Amnesty International were the first access to the leak containing a list of more than 50,000 phone numbers that were potentially targeted or sought to be targeted by NSO clients. The data also contains the time and date that numbers were selected, or entered onto a system. More than 1000 Indian numbers appeared on the list, and the Consortium was able to verify the identities of people associated with more than 300 of the numbers. True copies of the articles first breaking the story, written by The Guardian, The Washington Post, The Wire, and Forbidden Stories, all dated 18.07.2021, are annexed herewith as **Annexure P-22 (Pg. Nos. 412 to 458)**.

34. The presence of a number in the leaked list, alone, is not an indication of whether there was an attempt to infect the phone with spyware. However, forensic examinations of a sample of 67 mobile phones with numbers on the list found close correlations between the time and date of a number in the data and the start of Pegasus activity — in some cases as little as a few seconds. Out of the 67 mobile phones, Amnesty International, which provided technical analyses and forensic support, found that 23 devices were successfully infected and 14 showed signs of attempted penetration. For the remaining 30, the tests were inconclusive, in several cases because the handsets had been replaced. Fifteen of the phones were Android devices, none of which showed evidence of successful infection.

However, unlike iPhones, phones that use Android do not log the kinds of information required for Amnesty International's detective work. Three Android phones showed signs of targeting, such as Pegasus-linked SMS messages.

35. The forensic analysis involved reaching out to persons whose numbers were on the leaked list. Those who consented to have their phones examined, such as the Petitioners, had their mobile phone devices subjected to an examination. The examination searched for digital evidence left behind by the Pegasus spyware. Amnesty International, in its Forensic Methodology Report dated July 18, 2021, has described how, in the past, it has recognised Pegasus attacks through specific domain names and network infrastructure used to deliver the attacks. In this Report, Amnesty International examined records of process executions (a process is a program in action; when a program is in action or execution it passes through states/stages which is known as process execution) on potentially infected iOS devices. These process executions did not match any legitimate code created or released by Apple. However, Amnesty was able to match them with the process execution that was previously detected on infected phones. A true copy of Amnesty International's Forensic Methodology Report dated July 18, 2021 is annexed herewith as **Annexure P-23 (Pg. Nos. 459 to 512)**.

36. To independently confirm these findings, Amnesty International shared "backup copies" of three iPhones with

Citizen Lab, an interdisciplinary laboratory based at the Munk School of Global Affairs & Public Policy, at the University of Toronto. Amnesty Internal did not provide any additional context or information about the devices or the investigation was provided to Citizen Lab. Citizen Lab was able to verify that Amnesty International's forensic methodology correctly identified infections, using NSO's Pegasus software, in the four iPhones. They also determined that Amnesty's overall methodology to identify the infections was sound. A true copy of the Citizen Lab's independent peer review of Amnesty International's forensic methods dated 18.07.2021 is annexed herewith as **Annexure P-24 (Pg. Nos. 513 to 515)**.

37. NSO describes its customers as 60 intelligence, military and law enforcement agencies in 40 countries as reported by The Washington Post, in an article dated 18.07.2021. Therefore, by closely examining the pattern of targeting by individual clients in the leaked data, the Consortium was able to identify 10 governments believed to be responsible for selecting the targets: Azerbaijan, Bahrain, Kazakhstan, Mexico, Morocco, Rwanda, Saudi Arabia, Hungary, India, and the United Arab Emirates. A copy of The Washington Post's article dated 18.07.2021 is annexed herewith as **Annexure P-25 (Pg. Nos. 516 to 543)**.

38. In India, 155 names have been revealed to be a part of the list of 50,000 verified phone numbers on which the spyware attack, on behalf of NSO's client(s), may have been conducted. These include journalists, politicians,

government servants, opposition leaders and their aides, intelligence officers, human rights defenders, lawyers, scientists, businesspersons, and even a sitting judge of this Hon'ble Court. A true copy of The Wire's article, last updated on 28.07.2021, which contains an exhaustive list of the Indian names revealed by The Pegasus Project is annexed herewith as **Annexure P-26 (Pg. Nos. 544 to 567)**.

39. With respect to India, Amnesty International's Security Lab conducted a forensic analysis of mobile devices of 8 journalists which were sent for forensic analysis. It was confirmed that the mobile phones of (i) Paranjoy Guha Thakurta; (ii) S.N.M Abidi (Senior Journalist), (iii) Sushant Singh (Previously at Indian Express), (iv) M.K. Venu (Founder, The Wire), and (v) Siddharth Varadarajan (Founder, The Wire) were infected by the Pegasus Spyware. The degree of surveillance and hacking in the case of the Petitioners, however, is presently unknown, which only adds to their concerns. A true copy of the article titled "Revealed: How The Wire and Its Partners Cracked the Pegasus Project and What It Means for India" published in the Wire on 30 July 2021 is annexed herewith as **Annexure P-27 (Pg. Nos. 568 to 589)**.

40. Pegasus' deployment upon journalists, activists, political leaders, businessmen, scientists, among others, raises concern about the sanctity of the freedom of speech and expression in a constitutional democracy such as India. There have been a variety of news reports alleging that the Respondents and/or agencies/instrumentalities of State

controlled by it are responsible for the Pegasus infections and related invasion of privacy suffered by hundreds of Indian citizens including the Petitioners. It has been widely reported in the press that the Respondent and/or agencies/instrumentalities of State controlled by it have paid NSO a significant sum of money to obtain the Pegasus malware and deploy it against Indian citizens.

41. Post the revelations made by The Pegasus Project, on 18.07.2021, the Government has, so far, failed to provide an adequate response and has not categorically denied its involvement in illegal surveillance. On 18.07.2021, ANI published what was reported as the Government's official response to The Pegasus Project, even though the "response" did not carry a signature, date or any official letterhead or marking. As in 2019, the Government assured citizens of its commitment to free speech and adherence to lawful methods of surveillance. The statement did not categorically deny, or admit to, the Government's involvement in the illegal surveillance and hacking and instead labelled the revelations as "malicious", based on "conjectures and exaggerations". It was also mentioned that India has a system of lawful interception of communications under Section 5(2) of the Indian Telegraph Act, 1885, and Section 69 of the IT Act and that any interception, monitoring, or decryption of communications is done as per the established process. A true copy of the undated, unsigned response published by ANI on July 19, 2021 has been annexed herewith as **Annexure P-28 (Pg. Nos. 590 to 591)**.

42. That on the same day as the revelations by the Pegasus Project, i.e. on 18.07.2021, the Minister of Electronics & Information Technology, Shri Ashwini Vaishnaw made a statement, in the Rajya Sabha, pertaining to the use of Pegasus Spyware. The Hon'ble Minister, once again, did not categorically deny the use or authorisation of the Pegasus spyware by the Government or any of its agencies; the Government's response was similar to the Pegasus-related official statements made in 2019. Instead, he made two claims, namely, that mere *"presence of a number* [on the leaked database of 50,000 phone numbers] *does not amount to snooping",* and *"NSO has also said that the list of countries shown using Pegasus is incorrect and many countries mentioned are not even our clients"*. The Hon'ble Minister then proceeded to label the reports as "*sensationalisation*". He further made reference to India's established procedures of lawful surveillance and the Government's adherence to the same. A true copy of the statement of Shri Ashwini Vaishnaw dated July 18, 2021 released by the Press Information Bureau on July 22, 2021 has been annexed herewith as **Annexure P-29 (Pg. Nos. 592 to)**.

43. The next day, i.e. on 19.07.2021, the Hon'ble Home Minister Shri Amit Shah, in a press release, said:

> "*Aap chronology samajhiye! This is a report by the disrupters for the obstructers. Disrupters are global organisations which do not like India to progress. Obstructers are political players in India who do not*

want India to progress… The facts and sequence of events are for the entire nation to see. Today the monsoon session of Parliament has started. In what seemed like a perfect cue, late last evening we saw a report which has been amplified by a few sections with only one aim — to do whatever is possible and humiliate India at the world stage, peddle the same old narratives about our nation and derail India's development trajectory."

A true copy of the press release dated 19.07.2021 is annexed herewith as **Annexure P-30 (Pg. Nos. to 593)**.

44. That on 28.07.2021, dissenting BJP lawmakers and absentee Government officials forced the Parliamentary Standing Committee on Information Technology to indefinitely postpone a scheduled meeting on the Pegasus snooping allegations. They did this by refusing to sign the attendance register which ensured a lack of quorum. Forbes India, on 28.07.2021, reported

"*The drama continued Wednesday as the Parliamentary Standing Committee on Information Technology met to discuss The Pegasus Project. Eleven BJP members turned up for the meeting but refused to mark their attendance in the register. As a result, the required quorum of ten members could not be reached and the meeting could not be officially convened with just nine on-the-record members.*"

A true copy of the article in Forbes India dated 28.07.2021 is attached herewith as **Annexure P-31 (Pg. Nos. 594 to 596).**

45. While the Petitioners have no idea who is behind the Pegasus malware infection on their phones- the aforesaid stance taken by senior government functionaries has meant that the Petitioners are left in a position where their most basic fundamental rights, i.e. their right to life, their right to privacy and their right to free speech have clearly been curtailed in a completely illegal manner and far from investigating how this happened, the very Government that is meant to protect these rights refuses to issue a categorical statement to the effect that that the Union of India and/or its agencies have never purchased/licensed the Pegasus malware or even that they have never used it against journalists, advocates and human rights activists in India. In this context, the Petitioners have been left with no option but to approach this Hon'ble Court to ensure that no citizen of India is ever again put through what the Petitioners has been put through and to ensure that our Fundamental Rights remain sacrosanct.

46. On July 29, 2021, France's national cybersecurity agency, ANSSI confirmed the presence of Pegasus spyware on the phones of two journalists from the country's online investigative journal Mediapart, becoming the first official government agency to confirm the cyber-attacks using Pegasus. A true copy of the report dated July 30, 2021, titled "French Agency Confirms Pegasus Hack, First Government Agency To Do So", published by NDTV.com is available as **Annexure-P-32 (Pg. Nos. 597 to 598)**.

47. The Government of Israel, through its Ministry of Defence, visited the offices of the NSO Group and inspected the surveillance software. This was done to verify "to examine" security breach allegations against the company's Pegasus spyware, circulating in the global media. Reportedly, categorical findings in the same are yet to reached/declared. A true copy of the article dated July 30, 2021, titled ""Working In Full Transparency With Israel": Pegasus Maker On Raids" as published by NDTV.com is available as **Annexure-P-33 (Pg. Nos. 599 to 605)**.

48. In the above circumstances, aggrieved by the illegal hacking in India that have breached the Petitioners' fundamental rights under Articles 19 and 21 (along with reportedly those of hundreds of other Indian citizens), the Petitioners are preferring the present Writ Petition inter alia on the following grounds, which are urged in the alternative and without prejudice to one another:

GROUNDS:

A. BECAUSE hacking using military-grade technology such as Pegasus on a smartphone, which falls within the definitions of 'computer' and 'computer system' as under Section 2 of the IT Act, is *ex facie* illegal and violates Section 43(a), 43(b), 43(c) and 43(d) of the IT Act, as it involves accessing a computer / computer system by introducing a 'contaminant' or 'virus'; damaging the device and extracting data without permission of the owner of the device. Pegasus therefore is a 'computer virus' and a 'computer contaminant' as under the IT Act since it is

designed to attach itself to a targeted device, and then modify, record and transmit data from the targeted devices.

B. BECAUSE the use of Pegasus violates Section 66B of the IT Act, which punishes dishonest receiving of stolen computer resources, since 'data' is included in the definition of 'computer resources' under Section 2(k) of the IT Act.

C. BECAUSE use of Pegasus violates Section 72 of the IT Act, which imposes a penalty for breach of confidentiality and privacy, against any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person.

D. BECAUSE hacking through Pegasus cannot be classified as a form of legitimate or authorised surveillance permitted under Section 69 of the IT Act or even Section 5 of the Telegraph Act, read with the relevant Rules, as it goes much beyond the mere interception, monitoring, or decryption of messages. It falls entirely beyond the, arguably unconstitutional, existing regime of lawful surveillance and does not even offer the limited safeguards afforded therein to aggrieved persons.

E. BECAUSE besides clear breaches of the IT Act regime, use of a technology such as Pegasus in certain contexts can also

contribute to commission of offences and subverting the basis of various other laws of India, specifically the Whistle Blowers Protection Act 2014.

F. BECAUSE the creators of Pegasus have confirmed that they only provide the military-grade spyware to governments and therefore it is reasonable to presume that the use of this spyware to engage in hacking of computer / computer systems, including those owned by the Petitioners, bear connection with the Respondents and therefore are acts which this Hon'ble Court is competent to examine under the scope of its writ jurisdiction under Article 32 of the Constitution of India.

G. BECAUSE the Respondents have, thus far, failed to unequivocally refuse the assertions that it did not enter into contracts for purchase of Pegasus spyware or otherwise sanction its use, and therefore it is reasonable to assume that the hacking of the computer / computer systems, including those of the Petitioners, were the result of actions traceable to public servants, and it is incumbent upon Respondents to furnish information to identify the source of what it claims was an illegal executive action.

H. BECAUSE the unique and incomparable nature of harms posed by the state-sponsored illegal hacking of *inter alia* the Petitioners' smartphones are an *ex facie* violation of their fundamental rights under Articles 19 and 21 of the Constitution and the impugned acts have caused irreparable injury and harm that warrant payment of damages or other

rehabilitative measures to be imposed *qua* Respondents to secure and enforce the Petitioners' fundamental rights.

I. BECAUSE the Hon'ble Supreme Court of the United States in *Riley v. California 573 U.S. 373 (2014),* has recognised the unique role played by smartphones in the lives of individuals today. They are not merely telephones used for the purpose of communication but are "extensions" of the person itself, in which deeply personal and private information touching upon all aspects of an individual's life can be found. State-sponsored illegal hacking of smartphones of *inter alia* the Petitioners thus strike at the very heart of the rights secured under Articles 19 and 21.

J. BECAUSE under the existing legal regime governing surveillance in India, persons are denied adequate procedural safeguards for safeguarding their fundamental rights *inter alia* those guaranteed under Article 19 and 21. The existing legal regime governing lawful surveillance does not provide for any judicial oversight and relies upon a purely executive-driven system to prevent misuse. It is the existence of concentrated and centralized State power, rather than its actual or potential use that creates a chilling effect and leads to psychological restraint on the ability of citizens to think freely. This induces a change in behaviour, that is further violative of Article 21 of the Constitution. Hacking, which falls outside the limited set of safeguards afforded in cases of lawful surveillance, casts an even darker and nearly indelible shadow of intrusion upon persons and

renders the enjoyment of their fundamental rights impossible by aggrieved persons.

K. BECAUSE the chilling effect caused by surveillance in general, which is only worsened where illegal surveillance in the form of hacking is involved, was explained by Justice Subba Rao in his dissenting judgment in *Kharak Singh v State of UP* [subsequently approved in *Puttaswamy (Privacy)*]. Recognising it is impossible to show actual, tangible harm in the case of surveillance, Justice Subba Rao noted:

> "*The freedom of movement in clause (d) therefore must be a movement in a free country, i.e., in a country where he can do whatever he likes, speak to whomsoever he wants, meet people of his own choice without any apprehension, subject of course to the law of social control. The petitioner under the shadow of surveillance is certainly deprived of this freedom. He can move physically, but he cannot do so freely, for all his activities are watched and noted. The shroud of surveillance cast upon him perforce engender inhibitions in him and he cannot act freely as he would like to do. We would, therefore, hold that the entire Regulation 236 offends also Art. 19(1)(d) of the Constitution*."

L. BECAUSE the chilling effect caused by the surveillance framework in India was explained in the Justice Srikrishna Committee Report:

> "The design of the current legal framework in India is responsible for according a wide remit to

> intelligence and law enforcement agencies. At the same time, it lacks sufficient legal and procedural safeguards to protect individual civil liberties. Much intelligence- gathering does not happen under the remit of the law, there is little meaningful oversight that is outside the executive, and there is a vacuum in checks and balances to prevent the untrammeled rise of a surveillance society."

M. BECAUSE the absence of any mechanism whereby a citizen is informed that they have been placed under surveillance, post facto or at any point in the future, further adds to this environment of uncertainty, where the behaviour of a citizen is modulated by the chilling effect on the broad sweep of surveillance practices, rather than any actual notice of their privacy being infringed. Illegal and unlawful surveillance by hacking computer devices, as in the present case, does not even offer these limited procedural safeguards to an aggrieved individual. It is grossly in contravention of the privacy principles that have been endorsed by this Hon'ble Court in *Puttaswamy (I)* & *Puttaswamy (II)*, for hacking through the use of Pegasus lacks any sense of accountability or transparency and results in leaving the aggrieved persons without any scope for redressal.

N. BECAUSE hacking through technologies such as Pegasus, is not merely illegal but an affront to the invaluable fundamental rights of the Petitioners safeguarded by

Articles 19 and 21 of the Constitution and veritably erode these rights.

O. BECAUSE the kinds of harms presented by the illegal hacking by way of Pegasus-like technology is amplified in certain contexts, including but not limited to the context of press and journalistic freedom which is directly relevant to the Petitioners. Constant surveillance upon activists, journalists and reporters violates that right under Article 19(1)(a) and impinges upon the freedom that the press needs in order to provide impartial and unbiased coverage, uninfluenced by external factors other than the truth of the story. Surveillance upon journalists and reporters is not, and can never be considered, a reasonable restriction under 19(2) of the Constitution, since it attacks not any instance of speech made by a journalist but attacks the journalist themselves. The surveillance using Pegasus is used as a tool to gag, silence and suppress independent reporting and activism.

P. BECAUSE hacking the smartphone of the Petitioners herein through Pegasus tantamounts to rendering it impossible for them to exercise their freedom to exercise their professions on account of the constant and untraceable surveillance that it involves. Not only is the privacy of the Petitioners grossly violated, but also of the various sources that regularly and routinely converse with him and provide information. It also leaves the sources vulnerable to state reprisal, some of whom already come from marginalised communities or are otherwise already susceptible to state violence.

Q. BECAUSE the use of Pegasus not only lacks any legal basis, but the incomparable nature of the surveillance it brings leaves an affected individual such as the Petitioners entirely bereft of any legal recourse adequately addressing the panoply of harm and injury suffered by him on account of there being no data protection law existing in India as on date. The manner of fundamental rights violations has left no recourse to the Petitioners except to approach this Hon'ble Court for securing and enforcing his fundamental rights;

R. That the Petitioners crave leave to add, alter or delete from the grounds mentioned above.

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

PRAYER

In light of the above facts and circumstances, the Petitioners pray that this Hon'ble Court may be pleased to:

i. Declare that the installation and/or use of malware or spyware such as Pegasus is illegal and unconstitutional and is *ultra vires* Part III of the Constitution;
ii. Issue a direction, order or writ, including writ in the nature of *mandamus* directing the Respondents to produce and disclose to this Hon'ble Court and the Petitionerall materials and documents with respect to all investigation,

authorisation, and/or order(s) pertaining to the use of Pegasus on the Petitioner;

iii. Issue a direction, order or writ, including writ in the nature of *mandamus* directing the Respondents to take suitable steps to protect Indian citizens from the use of cyberweapons/malware such as Pegasus;

iv. Issue a direction, order or writ, including writ in the nature of *mandamus* directing the Respondents to put in place a judicial oversight mechanism to deal with any complaints on illegal breaches of privacy and hacking and punish all government officials responsible for such breaches; and

v. Pass such other and further order or order as may be deemed fit and proper in the interest of justice.

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

Place: New Delhi
Drawn on: 29.07.2021
Filed on: 31.07.2021

[redacted]
PRATEEK K. CHADHA
ADVOCATE FOR THE PETITIONERS

[redacted]