SYNOPSIS

1. Petitions have been filed in this Hon'ble Court regarding the Pegasus spyware, the role of the NSO, wide-spread illegal surveillance by Government bodies and private sector alike, the uncontrollable spread of the vice of snooping, illegal surveillance rendering the statutory provisions illusory and the concomitant effect of the right to privacy of the individual being routinely violated on a very large scale.
2. Having perused the petitions filed in court this petition will avoid the pleadings and documents relied upon in the earlier petitions unless repetition is absolutely necessary and relies on what is set out herein below.
3. First, this Petition is not merely about NSO and Pegasus but a challenge to India's communications surveillance mechanism that stands in contrast with the other democracies of the world for lack of any judicial or parliamentary oversight. India is the only democracy where communications surveillance continues to be the exclusive domain of the Executive arm of the Government with no provisions for public or judicial oversight of the surveillance process. Government of India are authorized under various statutes and license agreements to conduct surveillance on India's communications networks on a large number of broadly worded grounds ranging from protection of national security to preventing the spread of computer viruses. Pursuant to authority so derived, several state surveillance programs already keep a close tab on our

communication networks, and far more potent surveillance technologies are in the pipeline in varying stages of deployment including the large scale data-mining and profiling capabilities of secret surveillance systems such as the CMS, NETRA and NATGRID. When moratoriums on facial recognition and artificial intelligence are being announced by leading democracies and private parties around the world, GoI is marching forward openly using them on protestors. There are constant efforts through the use of subordinate legislation to break End to End encryption--the only defense available for secure communications. Phone tapping orders are so rampant that they no longer make the headlines. Government procures increasingly sophisticated technology enabling such surveillance from private companies often justifying them to be essential for maintaining law and order. But as we have been watching in addition to legitimate purposes, these technologies are used to shrink the space for political dissent, target our own citizens in violation of their internationally recognised human rights.

4. This Public Interest Litigation relies on the following expert reports, United Nations Documents and Judgments, and asks this Hon'ble Court to make orders and issue guidelines in respect of the recommendations made in these reports which include judicial oversight, the protection of the human right to privacy, transparency, the pernicious impact worldwide including in India of private surveillance technology companies, information to parties concerned regarding unlawful surveillance, and the like.

I. Committee/Law Commission Reports

a. Ireland Law Reforms Commission Report on Privacy: Surveillance and the Interception of Communication, Ireland, 1997 [ANNEXURE P-1]

b. The New South Wales Law Reform Commission Report 108 titled "Surveillance: Final Report" (May, 2005) [ANNEXURE P-2]

c. European Union Agency for Fundamental Rights (FRA) Report on "Surveillance by intelligence services - Volume I: Member States' legal frameworks" (18.11.2015) [ANNEXURE P-20]

d. Venice Commission Report on the Democratic Oversight of Signals Intelligence Agencies, 15.12.2015 [ANNEXURE P-21]

II. List of United Nations Documents:

a. UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc. A/RES/73/179 (17.12.2018)

b. UN General Assembly Resolution on the Protection of Human Rights and Fundamental Free

c. U.N. General Assembly Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/RES/73/179 (17 December 2018)

d. U.N. General Assembly Resolution on the Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, U.N. Doc. A/RES/72/180 (19

December 201

e. Concluding observations on the fifth periodic report of Belarus, Human Rights Committee, U.N. Doc. CCPR/C/BLR/CO/5 (22 November 2018)

f. Report of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age, U.N. Doc. A/HRC/39/29 (3 August 2018)

g. Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/27/37 (30 June 201

h. Concluding Observations on the Fourth Periodic Report of the Republic of Korea, Human Rights Committee, U.N. Doc. CCPR/C/KOR/CO/4 (3 December 2015

i. U.N. General Assembly Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/RES/73/179 (17 December 2018)

j. Concluding observations on the fifth periodic report of Belarus, Human Rights Committee, U.N. Doc. CCPR/C/BLR/CO/5 (22 November 2018

k. Report of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age, U.N. Doc. A/HRC/39/29 (3 August 2018)

l. Report of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age, U.N. Doc. A/HRC/39/29 (3 August 2018)

III. international decisions in respect of privacy and surveillance.

a. Maximillian Schrems v. Data Protection Commissioner, C-362/14, Advocate General's Opinion, 23 September 2015

b. Maximillian Schrems v. Data Protection Commissioner, C-362/14, 6 October 2015

c. Big Brother Watch and Others v. the United Kingdom, No. 58170/03, communicated on 9 January 2014

d. CJEU, Joined Cases C-203/15 and C-698/15, Tele2 Sverige and Watson v. Home Secretary, 21 December 2016

e. ECHR, Roman Zakharov v. Russia [GC], No. 47143/06, 4 December 2015,

LIST OF DATES

Date	Particulars
(1800-1979)	
1885	The Indian Telegraph Act was enacted by the British Raj in order to control and restrain the telegraph communications during the colonial era. The act continues to be in force till date and it allows Central government and the state governments to intercept messages
1898	The Indian Post Office Act was passed which allowed the British Raj to intercept postal articles. The act continues to be in force till date, allowing the Central and State governments to intercept posts in case of a public emergency or in the interest of public safety or tranquillity.
1973	The Criminal Procedure Code is amended and it brings two new sections namely section 91 and 92 which authorize the courts, police officials and district magistrates to summon any document or "thing" from any person, postal or telegraph authority or investigation, inquiries or trials.
(1980s)	
Aug 10, 1988	Ramakrishna Hegde, the then Chief Minister of Karnataka, resigned after being held responsible for tapping the telephones of journalists and rival politicians. Mr. Hegde denied his involvement in the bugging but accepted responsibility and he said that he was stepping down on moral grounds.
(1990s)	
February, 1990	India Today published a news report stating that a secret report by the CBI on telephone tapping which was ordered by the V.P. Singh government, contained

	details about phone tapping ordered by the Central government in the previous decade. The CBI report, reportedly said that the government headed by Congress (I) and the AIDMK, mostly between 1984 and 1987, had ordered the Intelligence Bureau to bug the phones of political opponents and also that of Central cabinet ministers, Congress MPs, MLAs, State ministers, trade unions and religious leaders.
1996	This Hon'ble Court in the landmark case of *People's Union for Civil Liberties (PUCL) vs. Union of India* (1997) 1 SCC 301, affirmed that tapping of telephones was a violation of the fundamental right to privacy and put in place guidelines ("PUCL Guidelines") that contained safeguards against arbitrariness in the exercise of the surveillance powers of the state.
1997	In what was considered to be the first instance of leak of a large volume of intercepted conversations in India, Conversations of industrialists Nusli Wadia, Ratan Tata and Keshub Mahindra were leaked. The Central government ordered a CBI inquiry into the audio tape leaks but subsequently it was closed for want of evidence. Conclusive answers as to who or which agency ordered the telephone taps on the industrialists, were never found.
(2009)	
Nov, 2009	In the aftermath of the 26/11 attacks in Mumbai, FICCI published a report titled "*FICCI Task Force Report on National Security & Terrorism"*. The report contained a set of recommendations on the counter-terrorism measures for the Central Government.
(2011)	

02.12.2011	Online news portal Medianama published an article titled "*Wikileak's SpyFiles on Digital Surveillance List 2 Indian Co's*". The article stated that the documents revealed by Wikileaks indicated that there were two Indian companies in the list of those providing digital surveillance technology. The two Indian companies mentioned in the article were "Shoghi" and "Clear Trail".
June, 2011	The then Finance Minister Mr. Pranab Mukherjee reportedly wrote a letter to the Prime Minister Manmohan Singh, voicing his concern about an adhesive-like substance which was recovered from his office, indicating a possible attempt to plant bugs in the office.
(2012)	
October, 2012	The Group of Experts on Privacy which was constituted by the Planning Commission under the Chairmanship of Justice A. P. Shah, submitted its Report. One of the problems highlighted by the report was the lack of a judicial oversight in the Indian Surveillance framework.
(2013)	
May, 2013	Edward Snowden, a former NSA/CIA subcontractor revealed around 10,000 documents to *the Guardian*, exposing various illegal mass surveillance programmes that were run by the Government of the United States in association with other state governments. The Snowden revelations gave information about the astounding scope of surveillance which was being carried out by the United States government on the citizens of a number of countries around the world, including India.

15.01.2013	Citizen Lab, a digital surveillance research group based out of Canada, published a report titled "*Planet Blue Coat Mapping Global Censorship and Surveillance Tools*". The Report elaborates upon a company called Blue Coat Systems which is a California based provider of network security and optimization products. The report further talks about "PacketShaper", a device that is capable of filtering, censorship and surveillance, was found in various countries including India.
13.03.2013	Citizens Lab published another report called "*For Their Eyes Only: The Commercialization of Digital Spying.*" which mentioned that a surveillance software called **FinFisher** which was created by a Munich based company Gamma International GmbH, was found on servers in India.
11.10.2013	The Central government amended the Unified Access License Agreement, in order to implement the Central Monitoring System (CMS).
(2014)	
08.01.2014	Petitioner No. 2 received a reply to an RTI which was filed seeking information on a Delhi Police tender, inviting technology companies to supply internet monitoring equipment. In 2011, the Provisioning & Logistics Department of the Delhi Police had issued a global notice inviting "expression of interest" from Indian and foreign technology companies to supply Internet monitoring equipment. Petitioner No. 2 then filed an RTI application before the Delhi Police in December 2013 seeking a list of companies that had responded to this notice. The response to the RTI revealed 26 Indian and

	foreign companies as having expressed interest in supplying monitoring equipment.
28.01.2014	The Ministry of Communications And Information Technology vide official Gazette Notification dated 28.01.2014 amended Rule 419A of the Indian Telegraph Rules 1951.
11.02.2014	In response to a question before the Lok Sabha on illegal tapping, the Minister of State in the Ministry of Home Affairs admitted that incidents of physical/electronic surveillance in the States of **Gujarat**, **Himachal Pradesh** and the **National Capital Territory of Delhi**, without authorization, had been reported.
2014	Petitioner No. 2 published a report titled "*India's Surveillance State"*. The report highlights several aspects of communication surveillance and the problems with the legal framework of surveillance in India.
12.05.2014	Reply to an RTI application sent by the Central Public Information Officer (**CPIO**), Ministry of Home Affairs received by the Petitioner No. 2 stating that 7500 to 9000 telephone tapping orders are issued by the Central Government every month.
18.12.2014	The Resolution on Right to Privacy in the Digital Age was adopted by the United Nations General Assembly.
(2015)	
04.03.2015	In response to a question before the Lok Sabha, the Minister of Communication said that on an average, 5000 interception orders are issued per month by the Union Home Secretary.
10.07.2015	Media house NDTV published an article titled "*UPA Was Client of Controversial Italian Spyware Firm, Claim Leaked Mails.*" The article points to a nexus between the

	Central Government and companies that sold software which was used for spying.
15.07.2015	The Economic Times published a news article titled "*Why Indian Intelligence uses small companies like Sunworks Consultants for spying technology*". The article elaborates upon a nexus between Indian Intelligence agencies and private entities, in the backdrop of obtaining surveillance technologies.
12.08.2015	In response to a question on the instances of illegal phone tapping, the then Minister of State in the Ministry of Home Affairs Shri Haribhai Paratibhai Chaudhary admitted that a few cases of illegal phone tapping had been registered in different police stations in Andhra Pradesh.
(2016)	
07.06.2016	The Hindu published/updated a news article titled "*India gets ready to roll out cyber snooping agency*", elaborating upon upon the setting up of the National Cyber coordination Center (NCCC) and highlighting the element of monitoring of internet (traffic) by the government.
21.08.2016	The Hindu published/updated an article detailing the findings of an investigation which was conducted by The Hindu, revealing that the internet activities of India's users were under surveillance and monitoring,
09.03.2012	The Hindu Businessline published/updated an article pointing out that an inter-ministerial panel had slammed the National Technical Research Organization (NTRO) for "*roping in a private company or setting the Internet monitoring system*" and the associated security concerns as the company was *selling similar solutions to other customers in the global market, thus not exclusive to India*".
(2017)	
24.08.2017	Hon'ble Supreme Court in **Justice K. S. Puttaswamy**

	(Retd.) and Anr. vs Union Of India And Ors held that the Right to Privacy under Article 21 of the Constitution of India is a fundamental right..
(2018)	
27.07.2018	The Justice BN Srikrishna Committee submitted its report titled "*A Free and Fair Digital Economy*, *Protecting Privacy*, *Empowering Indians*" to the Union Minister for Electronics and IT, law and Justice Shri Ravi Shankar Prasad.
18.09.2018	Citizen Lab's, a Toronto based digital surveillance research group, published a report titled "**Hide And Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries**", revealing the use of Pegasus malware/spyware was used to conduct surveillance across 45 Countries, including India.
(2019)	
19.02.2019	Petitioner No. 2 sent its submissions on "The Surveillance Industry and Human Rights" to Mr. David Kaye, Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression.
17.05.2019	CERT.in issued a vulnerability note about a "Buffer Overflow Vulnerability in WhatsApp." The note said that an attacker could exploit the said vulnerability to target a user's phone number, could access information on the system and compromise it.
28.05.2019	The UN Special Rapporteur presented a report on the adverse effect of the surveillance industry on freedom of expression (A/HRC/41/35) to the United Nations Human Rights Council. The report talks about targeted surveillance and the regulation of public-private collaboration in the sale, transfer, use and after-sales

	support of surveillance technologies.
24.06.2019	The Citizen Lab published an article titled "***The Dangerous Effects of Unregulated Commercial Spyware***" highlighting a chilling trend wherein political opponents, Human Rights organizations and Lawyers, journalists and members of civic media were disproportionately targeted with powerful spyware technologies.
05.09.2019	WhatsApp wrote a letter to CERT-In, conveying information in respect of an incident that had occurred in May, 2019 wherein the devices of 121 users in India "*may have been attempted to be reached*". CERT-In reportedly sought more details from WhatsApp in relation to the said incident.
19.09.2019	Hon'ble Kerala High Court in **Faheema Shirin R.K. v. State of Kerala &Ors** W.P. (C) No. 19716 of 2019 (L) held Right to Internet Access a fundamental right under Right to Education and Right to Privacy. The 3rd Petitioner intervened in the writ petition in support of the petitioner.
22.10.2019	The Bombay High Court interpreted Section 5(2) of the Telegraph Act, 1885 in light of the *Puttaswamy* (Privacy-9J) judgment and ordered for the destruction of the documents produced as evidence that was collected through surveillance, done unconstitutionally and thus not admissible in court. It applied the proportionality standards to the surveillance order and concluded that CBI didn't pass muster for lacking legal basis and not meeting the standard of least restrictive means to infringe privacy.
01.11.2019	News Media house 'The Quint' published an article titled "*Govt Knew NSO, Other Spyware Firms Operated in*

	India: Ex-Home Secy" The article quotes former home secretary GK Pillai as saying that he was aware that Israeli Tech firm NSO had been operating in India and that it had sold spying software to private firms and individuals in the country. The article states: "*Former home secretary GK Pillai told The Quint on Friday, 1 November, that he is aware that Israeli tech firm NSO had been operating in India – and that it had sold spying software to private firms and individuals in the country. He also confirmed that Indian government agencies have bought spyware in the past from private foreign tech firms like NSO. In fact, he said, "it is quite common."*
19.11.2019	A group of 19 lawyers and activists wrote a letter to the Central Government, mentioning that they had been targeted by Pegasus and further asking if the taxpayers' money had been put to use for conducting surveillance of such nature
13.11.2019	Facebook published its Transparency Report for the period January-June, 2019 which shows that between January to June 2019, 22,684 requests for user data were received by Facebook from the Indian Government agencies.
19.11.2019	The Petitioner No. 1 along with 16 other individuals who had been targeted by the NSO-Pegasus Spyware, sent a letter to the Parliamentary Standing Committee on Information Technology, highlighting the fact that they had received communication from WhatsApp and Citizen Lab, informing them that their mobile devices had been targets of highly sophisticated cyber attacks.

	The letter further requested the Standing Committee to take oral testimony to the Committee and to conduct a thorough probe, report on the same and ensure that appropriate action was taken.
04.12.2019	Unstarred Question No. 2576 asked in the Lok Sabha as to whether the Government has assessed the extent of privacy breaches in the WhatsApp snooping by the Pegasus Software and whether any theft of private data of the citizens had taken place. Hon'ble Union Minister of Electronics and Information Technology answered the question stating that the full extent of this attack may never be known. It is also believed that it is likely that personal data within the WhatsApp app of approximately twenty users may have been accessed out of approximately one hundred and twenty-one users in India whose devices the attacker attempted to reach.
(2020)	
05.05.2020	The Quint, a prominent media house in India, published an article titled "*Govts Deployed Pegasus Spyware on People: NSO Group Tells US Court*". The article quotes Former home secretary GK Pillai saying **-** "***he is aware that Israeli tech firm NSO had been operating in India – and that it had sold spying software to private firms and individuals in the country***."
(2021)	
19.07.2021	news media house The Wire published a series of reports, containing startling revelations about the use of Pegasus on a number of Indian Citizens.
19.07.2021	The UN High Commissioner for Human Rights Michelle Bachelet issued a statement on the Pegasus issue. The statement warned about the dangers of the use of the

	Pegasus software, acknowledged its misuse and the implications on free speech and human rights and reminded the states that surveillance can only be used in “narrowly justified circumstances.”
09.08.2021	Hence this Petition.

IN THE SUPREME COURT OF INDIA

CIVIL ORIGINAL JURISDICTION

WRIT PETITION (CIVIL) NO. _____ OF 2021

(PUBLIC INTEREST LITIGATION)

IN THE MATTER OF:

DEGREE PRASAD CHAUHAN & OTHRS. ...PETITIONERS

Versus

UNION OF INDIA & OTHERS ...RESPONDENT

1.	Degree Prasad Chouhan [redacted]	...Petitioner No. 1
2.	Software Freedom Law Center, India (SFLC.in) Through its Operations Lead Mamta Verma, K-9, Jangpura Extension New Delhi PIN - 110014	...Petitioner No. 2
Versus		
1.	Union of India Through its Secretary, Ministry of Home Affairs North Block New Delhi- 01	...Respondent No.1

2.	Ministry of Electronics & Information Technology, Through its Secretary Room No. 655, A-wing, Shastri Bhawan, New Delhi- 01	...Respondent No. 2
3.	Indian Computer Emergency Response Team (CERT-In) Through its Secretary, (Ministry of Electronics and Information Technology, Government of India) Electronics Niketan 6, CGO Complex, Lodhi Road, New Delhi - 110 003 India Ph. : 91-11-23379885	...Respondent No. 3
4.	Govt. of NCT of Delhi Through the Chief Secretary, Govt. of NCT of Delhi, Delhi Secretariat, New Delhi	...Respondent No. 4
5.	State of Meghalaya Through the Chief Secretary, Government of Meghalaya, Shillong-793001	...Respondent No. 5
6.	State of Maharashtra Through the Chief Secretary, Government of Maharashtra, Mantralaya, Mumbai-400032	...Respondent No. 6
7.	State of Haryana Through the Chief Secretary, Government of Haryana, Chandigarh-160001	...Respondent No. 7

8.	State of Uttar Pradesh Through the Chief Secretary, Krishi Bhawan, Madan Mohan Malviya Marg Lucknow-226001.	...Respondent No. 8
9.	State of Bihar Through the Chief Secretary, Government of Bihar, Main Secretariat Building, Patna - 800015	...Respondent No. 9
10.	State of Assam Through the Chief Secretary, Government of Assam, P.O. Assam Sachivalaya, Guwahati - 781006	...Respondent No. 10
11.	State of Andhra Pradesh Through the Chief Secretary, AP Secretariat Office, Velagapudi	...Respondent No. 11
12.	Union Territory of Jammu and Kashmir Through the Chief Secretary, Government of Jammu & Kashmir, Srinagar-190001	...Respondent No. 12
13.	Union Territory of Ladakh Through the Chief Secretary Government of UT of Ladakh	...Respondent No. 13
14.	State of Chhattisgarh Through the Chief Secretary, Government of Chhattisgarh, Mahanadi Bhawan, Mantralaya, Naya Raipur-492002	...Respondent No. 14

15.	State of Himachal Pradesh Through the Chief Secretary, Government of Himachal Pradesh, Shimla-171002	...Respondent No. 15
16.	State of Odisha Through the Chief Secretary, Government of Odisha, Bhubaneshwar-795001	...Respondent No. 16
17.	State of Madhya Pradesh Through the Chief Secretary, Government of Madhya Pradesh, Bhopal-462004	...Respondent No. 17
18.	State of Arunachal Pradesh Through the Chief Secretary, Government of Arunachal Pradesh, Itanagar-791111	...Respondent No. 18
19.	State of Gujarat Through the Chief Secretary, Government of Gujarat, 5th Floor, Sardar Bhawan, Sachivalaya, Gandhinagar-382010	...Respondent No. 19
20.	State of Manipur Through the Chief Secretary, Government of Manipur, Old Secretariat, Bapupara, Imphal- 795001	...Respondent No. 20
21.	State of Mizoram Through the Chief Secretary, Government of Mizoram, Aizawl-796001	...Respondent No. 21

22.	State of Nagaland Through the Chief Secretary, Government of Nagaland, Kohima – 797001	...Respondent No. 22
23.	State of Punjab Through the Chief Secretary, Government of Punjab, Chandigarh-160001	...Respondent No. 23
24.	State of Rajasthan Through the Chief Secretary, Government of Rajasthan, Jaipur-302005	...Respondent No. 24
25.	State of Sikkim Through the Chief Secretary, Government of Sikkim, New Secretariat, Development Area, Gangtok-737101	...Respondent No. 25
26.	State of Tamil Nadu Through the Chief Secretary, Government of Tamil Nadu, Chennai-600009	...Respondent No. 26
27.	State of Tripura Through the Chief Secretary, Government of Tripura, New Secretariat Complex, Agartala– 799011.	...Respondent No. 27
28.	State of Uttarakhand Through the Chief Secretary, Government of Uttarakhand, Dehradun-248001.	...Respondent No. 28
29.	State of West Bengal Through the Chief Secretary, Government of West Bengal, Kolkata-700001.	Respondent No. 29

30.	State of Kerala Through the Chief Secretary, Government of Kerala, Thiruvananthapuram, Kerala-695001	...Respondent No. 30
31.	State of Jharkhand Through the Chief Secretary, 1st Floor, Project Building, Dhurwa, Ranchi, Jharkhand 834004	...Respondent No. 31
32.	Union Territory of Goa Through the Chief Secretary, Government of Goa Secretariat, Porvorium-403521	...Respondent No. 32
33.	Union Territory of Chandigarh Through the Chief Secretary, 4th floor, Civil Secretariat, Chandigarh	...Respondent No. 33
34.	Union Territory of Puducherry Through the Chief Secretary Govt. of Puducherry, Chief Secretariat, Goubert Avenue, Puducherry- 605001	...Respondent No. 34
35.	Union Territory of Andaman & Nicobar Islands Through the Chief Secretary, Andaman & Nicobar Administration Secretariat, Port Blair.	...Respondent No. 35
36.	Union Territory of Dadra & Nagar Haveli Through its Administrator Govt. of Dadra & Nagar Haveli, U.T., Secretariat, Silvassa, Nagar Haveli- 396230	...Respondent No. 36

37.	Union Territory of Daman & Diu Through the Chief Secretary UT of Daman & Diu, Daman	...Respondent No. 37
38.	Union Territory of Lakshadweep Through the Chief Secretary UT of Lakshadweep Secretariat, Kavaratti 682555	...Respondent No. 38
39.	State of Telangana Through the Chief Secretary Basheerbagh, Hyderabad	...Respondent No. 39
40.	State of Karnataka Through the Chief Secretary, Room No.222, II Floor, VidhanaSoudha, Bengaluru, Karnataka- 560001	...Respondent No. 40

TO,

THE HON'BLE CHIEF JUSTICE AND HIS

OTHER COMPANION JUSTICES OF THE HON'BLE

SUPREME COURT OF INDIA

THE HUMBLE PETITION OF

THE PETITIONER HEREIN

MOST RESPECTFULLY SHOWETH THAT:

1. The present Public Interest Litigation has been filed by the Petitioners in public interest under Article 32 of the Constitution of India seeking *inter alia* the issuance of the writ of Mandamus or any other appropriate order or direction, directing the Respondent No. 1 to 40, to

take certain steps to ensure the protection of Fundamental Rights guaranteed to the citizens under the Constitution of India, in the backdrop of the Pegasus Surveillance issue in India. Petitioner No. 1 is aggrieved but he has approached this Hon'ble Court in public interest and he is not seeking any relief for himself. Petitioner No. 2 is a civil society organization that works on digital rights and has approached this Hon'ble Court in public interest.

1A. The Petitioners have not approached any other authority for the same relief.

Parties

2. That Petitioner No. 1 is a human rights defender, a journalist, a lawyer and an activist. He has been working at the grassroots level for the upliftment and protection of rights of Dalits and Indigenous communities in Chhattisgarh, for the past 15 years. He is the convenor of Adivasi Dalid Majdoor Kisan Sangharsh, a community group set up by Adivasi villagers to respond to the alleged unlawful dispossession of their land by two companies. He also serves as the Vice President of the Chattisgarh chapter of the People's Union for Civil Liberties, one of India's oldest human rights organizations. In 2019, Petitioner No. 1 was informed by the Citizen Lab that he was spied on through his mobile phone. He had also received a communication from WhatsApp informing him that his privacy had been breached. The Petitioner is the Son/Daughter of Mr. Gulapa Chouhan, residing at [redacted]. The

Petitioner's Annual income is approximately [redacted]. By virtue of his activism and work for the downtrodden, Petitioner No. 1 has faced several interrogation sessions by law enforcement authorities which did not culminate into a trial. He has also been implicated into a number of false or fabricated cases and he has been acquitted in almost all of them. Although the Petitioner No. 1 is an aggrieved party, he has approached this Hon'ble Court in public interest and is not seeking any relief for personal interest or for himself.

3. That Petitioner No. 2 is a registered society under the Societies Registration Act, 1860 bearing registration number S-68628 dated 03-03-2010. Petitioner No. 2 has an annual income of approximately Rs. [redacted] Petitioner No. 2 works for the promotion and protection of digital rights and digital freedoms and it has intervened and filed legal actions before various courts, nationally and internationally, seeking protection of individual privacy, right to Internet access, and protection of freedom of speech and expression online. Petitioner No. 2 has researched and published multiple reports exploring the laws and rights relating to the freedom of speech and expression, Internet shutdowns, online harassment, intermediary liability, and tracks instances of violation of freedom of speech and expression through censorship in the country. Pertaining to the issue at hand, Petitioner No. 2 in 2014 had published a report titled “India’s Surveillance state” which delves into communication surveillance in India, the relevant legal provisions and the international human rights principles. The said report was circulated and quoted widely by various stakeholders. Petitioner No. 2 has relentlessly pursued the protection of privacy rights of Indian

citizens. In furtherance of its advocacy efforts, it has filed a number of RTIs leading to disclosure of important information. In 2019, it had also sent its submissions titled “The Surveillance Industry and Human Rights” to the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, when the Special Rapporteur had invited comments on the surveillance industry and human rights.

4. Respondent No. 1 is the ministry of the Union Government which is responsible for issuing interception Orders and also responsible for maintaining internal security in India, among other responsibilities. Respondent No. 2 is responsible for policy matters relating to information technology; Electronics; and Internet (all matters other than licensing of Internet Service Provider); and is also responsible for the promotion of internet, IT and IT enabled services.

5. Respondent No. 3 is a government mandated information technology security organization. It is a division under Respondent No. 2 and it is the national nodal agency for responding to computer security incidents in India, as and when they occur.

6. Respondents No. 4- 30 are the State Governments and the Union Territories.

7. That, the present petition under Article 32 of the Constitution of India is being filed by way of Public Interest Litigation and the Petitioners have no personal interest herein. Although Petitioner No. 1 is aggrieved but he approaching this Hon'ble Court in public interest and is not seeking any relief for himself. This petition is being filed in the interest of the public

at large and with a view to seek certain reliefs from the Respondents for the public at large, in light of the Pegasus surveillance issue.

8. That the Petitioners are filing the present Petition on their own and the litigation cost is being borne by the Petitioners.

9. That, a thorough research has been conducted in the matter raised through the present Writ Petition/PIL and the relevant available matters in this regard are being annexed herewith.

10. That, to the best of the Petitioner's knowledge and research, the issue raised herein was not dealt with or decided by this Hon'ble Court and that a similar or identical petition was not filed earlier by the Petitioners.

11. That In 2019, the Petitioner No. 2 along with the Center for Public Interest Litigation (CPIL), had filed a Writ Petition praying for an order directing the government to stop the operation of surveillance projects namely Central Monitoring System (CMS), National Intelligence Grid (NATGRID) and Network Traffic Analysis (NETRA) and for setting up an independent judicial and/or parliamentary oversight body for issuing and reviewing interception Orders.

12. **OVERVIEW OF SURVEILLANCE LAWS OF FOREIGN JURISDICTIONS**

It is important to highlight the shortcomings in the Indian lawful interception and monitoring framework, by contrasting its features with the safeguards in other legal systems.

I. UNITED STATES OF AMERICA

A. The Wiretap Act

- Bans the use of certain electronic techniques by private citizens and requires government officials to obtain a court order before utilizing electronic techniques such as wiretaps. The Federal Law enforcement must obtain internal approval to seek a court order authorizing interception from specified senior officials within the DOJ.
- After obtaining internal approval, federal agents must apply for and obtain an Order from a federal court to intercept wire, oral, or electronic communications unless there is an emergency involving immediate danger or death or serious bodily injury to any person.
- Government must obtain a court order authorizing and approving the emergency interception within 48 hours after interception occurs or begins to occur.
- The Government's application to the judge must also satisfy the judge that the other less intrusive investigative procedures have been tried without success, would not be likely to succeed or would be too dangerous to use.
- The judicial order is not valid for more than 30 days but an extension on the same can be granted.
- During the period of the Order, agents have a continued duty to minimize i.e. not record or overhear conversations that are not related to the crimes or persons for which the order was obtained. The recordings have to be further sealed in a manner that will protect them from tampering.

B. Electronic Communications Privacy Act (ECPA), 1986

- Applies to access to stored wire and electronic communications and transactional records.

C. PATRIOT Act, 2001

- Federal agents are allowed to use multi-point wiretaps but with a court approval, to investigate international terrorists who are trained to evade detection.

D. Homeland Security Act of 2002

- Requires the appointment of a Chief Privacy Officer at the Department of Homeland Security.

E. United States Foreign Intelligence Surveillance Court FISA Courts or FISC

- In 1978, the United States of America established the FISC by enacting The Foreign Intelligence Surveillance Act of 1978 that prescribes procedures for requesting judicial authorization for electronic surveillance and physical search of persons engaged in espionage or international terrorism against the United States on behalf of a foreign power. Requests are adjudicated by a special eleven member court called the Foreign Intelligence Surveillance Court.
- This was a result of extensive investigations by Senate Committees into the legality of domestic intelligence activities as a response to President Richard Nixon’s usage of federal resources, including law enforcement agencies, to spy on political

and activist groups. India seems to be at the same exact inflection point.

- The Foreign Intelligence Services Act established the FISA Courts which consists of 11 district court judges. The judges are chosen publicly by the Chief Justice of the United States and are drawn from seven of the federal judicial circuits.
- Applications under FISA are heard by a FISC judge and as per the law, the government cannot ask a second judge to decide on an application for electronic surveillance after one FISC judge has denied it.
- An appeal from the FISA Court lies with the Foreign Intelligence surveillance Court of Review.

F. Other Safeguards

- Officer of the Director of National Intelligence (DNI) has a dedicated Civil Liberties Protection Officer who oversees intelligence programs.
- The US Intelligence community is required to report to Congress on its programs and activities where there are debates on such issues.
- The Obama administration conducted a broad-ranging and unprecedented review of the US Signals Intelligence Programs between 2013-2014. The process of review took inputs from major stakeholders as well as the President's Review Group on Intelligence and Communications Technologies, Congress, the Tech Community, civil society, foreign partners, Privacy and Civil

Liberties Oversight Board and others. The objective of the review process was to use intelligence capabilities in a manner that protects national security while respecting privacy and civil liberties.

- Subsequently in 2014, President Obama announced several reforms and issued a Presidential Policy Directive on Signals intelligence activities. (Source: OCHR Website)

13. **REPORTS FROM DIFFERENT JURISDICTIONS**

Following is a list of the relevant extracts and summarized points, from country wide commission and committee reports and United Nations documents on Surveillance.

1. **Venice Commission Report on the Democratic Oversight of Signals Intelligence Agencies Adopted by the Venice Commission at its 102nd Plenary Session (Venice, 20-21 March 2015)** [ANNEXURE P-21]

Background: Initially in 2007, in response to an invitation of the Committee of Ministers of the Council of Europe, the European Commission for Democracy through Law (Venice Commission) adopted a report on the Democratic Oversight of the Security Services. In November, 2012, the Committee on Legal Affairs and Human Rights of the Parliamentary Assembly of the Council of Europe placed a request with the Venice Commission to prepare a update of the earlier report. Subsequently, the updated version of the report was discussed in a meeting with the Sub-commission of Democratic Institutions on 19th

March 2015 and the same was then adopted by the Venice Commission in its 102nd Plenary Session. The report was published on 15.12.2015.

Important Pointers:

- "*Signals intelligence has a very large potential for infringing privacy and certain other human rights. Understanding strategic surveillance merely through the lens of the right to privacy may not completely capture its potential harm. Unlike the situation for rendition, where the harm is clear, immediate and individualised, the damage insufficiently regulated and controlled signals intelligence can do to society is more diffuse and long term. The existing situation can result in competing or incompatible obligations being placed on companies (typically disclosure vs. data protection) and in circumvention of stronger domestic telecommunications surveillance procedures. Agreement on minimum international standards on privacy protection thus appears to be necessary.*" (Para 128)

- "*Signals intelligence can be regulated in a lax fashion, meaning that large numbers of people are caught up in a net of surveillance, or relatively tightly, meaning that the actual infringement of individuals' privacy and other human rights is more limited. For parties to the ECHR, it is necessary in any event to regulate the main elements of signals intelligence in statute form.* ***The national legislature must be given a proper opportunity to understand the area and draw the necessary balances****. However, European states should not be content with*

satisfying the quality of law standards of the ECHR. ***Only strong independent control and oversight mechanisms can assuage public concern that signals intelligence is not being abused***." (Para 129)

2. **European Union Agency for Fundamental Rights (FRA) Report on "Surveillance by intelligence services - Volume I: Member States' legal frameworks"** [ANNEXURE P-20]

Background: In response to the Snowden revelations, the European Parliament passed a resolution which among other aspects, asked the European Union Agency for Fundamental Rights to undertake a research on the fundamental rights protection in the context of surveillance and the available remedies. The report is a step by the FRA in response to the European Parliament's request. It gives an overview of the legal framework of the EU member states in respect of surveillance. This report draws on data provided by the agency's multidisciplinary research network 'Franet', which were collected through desk research in all the 28 EU Member States, based on a questionnaire submitted to the network. The Report aims to support the implementation of oversight mechanisms in the EU and its Member States. It does so by analysing the legal frameworks on surveillance in place in different EU Member States, focusing on 'mass surveillance', which has a high potential for abuse. The Report was published on 18.11.2015.

Important Pointers:

- *"The general consensus, taken from the Venice Commission report and academic studies, is that oversight should be a combination of executive control; parliamentary oversight; judicial review; and expert bodies.*" (Chapter 2)

- *"UN good practices on oversight institutions - Practice 6. Intelligence services are overseen by a combination of internal, executive, parliamentary, judicial and specialised oversight institutions whose mandates and powers are based on publicly available law. An effective system of intelligence oversight includes at least one civilian institution independent of both the intelligence services and the executive. The combined remit of over-sight institutions covers all aspects of the work of intelligence services, including their compliance with the law; the effectiveness and efficiency of their activities; their finances; and their administrative practices.*

  Practice 7. Oversight institutions have the power, re-sources and expertise to initiate and conduct their own investigations and have full and unhindered access to the information, officials and installations necessary to fulfil their mandates. Oversight institutions receive the full co-operation of intelligence services and law enforcement authorities in hearing witnesses and obtaining documentation and other evidence. UN, Human Rights Council, Scheinin, M. (2010)"

- *"UN good practice on complaints and effective remedy- Practice 9. Any individual who believes that her or his rights have*

been infringed by an intelligence service can bring a complaint to a court or oversight institution, such as an ombudsman, human rights commissioner or national human rights institution. Individuals affected by the illegal actions of an intelligence service have recourse to an institution that can provide an effective remedy, including full reparation for the harm suffered. UN, Human Rights Council, Scheinin, M. (2010) (Chapter 3: Remedies)"

3. **Report on Privacy: Surveillance and the Interception of Communications IRELAND (1997)** [ANNEXURE P-1]

Background: The Law Reform Commission in Ireland was established by section 3 of the *Law Reform Commission Act, 1975* on 20th October, 1975. It is an independent body consisting of a President and four other members appointed by the Government. The Report by the Law Reform Commission on "*PRIVACY: Surveillance and the Interception of Communications*" consists of Ireland's Law Reform Commission's final recommendations with respect to privacy in the specific context of surveillance and the interception of communications. The Report also contains the privacy problem posed by surveillance in all contexts.

Important pointers and Recommendations:

- The report acknowledges that Privacy is not merely instrumental to the achievement of other goals but is a basic human right that applies to all persons in virtue of their status as human beings. It

further states that privacy is "*an organising principle of civil society."* (Para 1.13, Chapter 1)

- On the point of involvement of private companies in surveillance, the report states as follows:

  "*The ongoing process of economic deregulation has dispersed this technology widely into private hands with the result that traditional legal protections that focus almost exclusively on the State as the sole potential abuser miss a large part of their target. Non-State actors pose just as much a threat as the State itself. The demand for such technology by private actors seems set to grow and not diminish. Restricting this market using traditional tools like import controls, a licensing regime for vendors, a licensing regime for users, etc., is unwieldy and likely to be piecemeal and ineffective*." (Para 1.69, Chapter 1)

- *"**Core Recommendation – tort of privacy-invasive surveillance:** the enactment of a new statutory tort to protect against the invasion of privacy by means of surveillance subject to certain conditions and defences."* [Para 1.80 (a)]

- ***"Provision of a basis in positive law for police surveillance of private places:** recommendation that, notwithstanding the provisions mentioned at B above, there should be a procedure for authorisation by warrant, by a Chief Superintendent for an initial short period and by a District Judge thereafter, for police surveillance (involving optical or hearing devices) of private places where this is justified for the prevention or detection of any crime in respect of which a search warrant may be issued under*

any statute or for the purposes for which a search warrant may be obtained under the Criminal Assets Bureau Act, 1996. ***Criteria should be laid down concerning the necessity for the surveillance and the justification for it including the likely impact of the surveillance on the rights of any person****. Supplementary provisions should be enacted regarding the use which may be made of information gained.*" [Para 1.80 (c)]

4. **New South Wales Law Reform Commission Report 108 "Surveillance: Final Report" May, 2005** [ANNEXURE P-2]

Background: In October 1996, the then Attorney General of Australia, JW Shaw, QC MLC, asked the Commission to inquire into and report on the scope and operation of the Listening Devices Act 1984, the need to regulate the use of visual surveillance equipment and any related matters thereto.

Recommendations:

Some of the major recommendations in the report include the following:

- *"With respect to the regulation of overt surveillance, the Privacy Commissioner should have the following powers and functions:*

  i. promoting, and providing assistance (eg, educational) for, compliance with the Overt Surveillance Principles;

  ii. assisting surveillance users in drafting codes of practice;

  iii. appointing inspectors to investigate complaints, and to conduct both routine and random inspections of surveillance

systems or devices to ascertain compliance with the proposed Act;

iv. *right of entry to non-residential premises to inspect surveillance systems or devices to ascertain compliance with the proposed Act;*

v. *educating the public on the acceptable use of surveillance devices.*"

(Recommendation 2)

- "*In determining whether to grant an authorisation to conduct covert surveillance in the public interest, the issuing authority should have regard to:*

  i. *the nature of the issue in respect of which the authorisation is sought;*

  ii. *the public interest (or interests) arising from the circumstances;*

  iii. *the extent to which the privacy of any person is likely to be affected;*

  iv. *whether measures other than covert surveillance have been used or may be more effective;*

  v. *the intended use of any information obtained as a result;*

vi. *the role played by the media in upholding the public interest; and*

vii. *whether the public interest (or interests) involved justifies the displacement of individual privacy in the circumstances.*"

(Recommendation 3)

5. **United Nations Documents**

Given below is a list of UN Documents on surveillance and the extracts therein:

A. U.N. General Assembly Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/RES/73/179 (17 December 2018)

"*Noting in particular that surveillance of digital communications must be consistent with international human rights obligations and must be conducted on the basis of a legal framework, which must be publicly accessible, clear, precise, comprehensive and non-discriminatory, and that any interference with the right to privacy must not be arbitrary or unlawful, bearing in mind what is reasonable with regard to the pursuance of legitimate aims, and recalling that States that are parties to the International Covenant on Civil and Political Rights must take the necessary steps to adopt laws or other measures as may be necessary to give effect to the rights recognized in the Covenant,"*

(ANNEXURE P-27, at Pg. 1046)

B. U.N. General Assembly Resolution on the Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, U.N. Doc. A/RES/72/180 (19 December 2017)

" "*5. Urges States, while countering terrorism:*

... (i) To safeguard the right to privacy in accordance with international law, in particular international human rights law, and to take measures to ensure that interferences with or restrictions on that right are not arbitrary, are adequately regulated by law and are subject to effective oversight and appropriate redress, including through judicial review or other means;

(j) To review their procedures, practices and legislation regarding the surveillance and interception of communications and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law, and to take measures to ensure that interference with the right to privacy is regulated by law, which must be publicly accessible, clear, precise, comprehensive and non-discriminatory, and that such interference is not arbitrary or unlawful, bearing in mind what is reasonable for the pursuance of legitimate aims;" "

(ANNEXURE P-27, at Pg. 1046)

C. Concluding observations on the fifth periodic report of Belarus, Human Rights Committee, U.N. Doc. CCPR/C/BLR/CO/5 (22 November 2018)

"*43. The Committee is concerned at reports that legislation provides for broad powers of surveillance and that the interception of all electronic communications, including through the system of operative investigative measures, which allows remote access to all user communications without notifying providers, does not afford sufficient safeguards against arbitrary interference with the privacy of individuals (art. 17).*

44. The State party should ensure that: (a) all types of surveillance activities and interference with privacy, including online surveillance for the purposes of State security, ***are governed by appropriate legislation that is in full conformity with the Covenant, in particular article 17, including with the principles of legality, proportionality and necessity, and that State practice conforms thereto****; ...*"

(ANNEXURE P-27, at Pg. 1046)

D. Report of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age, U.N. Doc. A/HRC/39/29 (3 August 2018)

"35. The law must be publicly accessible. Secret rules and secret interpretations of law do not have the necessary qualities of "law" (ibid., para. 29). Laws need to be sufficiently precise. Discretion granted to the executive or a judge and how such discretion may be exercised must be circumscribed with reasonable clarity (see A/69/397, para. 35). To that end, the nature of the offence and the category of persons that

may be subjected to surveillance must be described. ***Vague and overbroad justifications, such as unspecific references to "national security" do not qualify as adequately clear laws. Surveillance must be based on reasonable suspicion and any decision authorizing such surveillance must be sufficiently targeted. The law must strictly assign the competences to conduct surveillance and access the product of surveillance to specified authorities***.

36. In terms of its scope, the legal framework for surveillance should cover State requests to business enterprises. It should also cover access to information held extraterritorially or information-sharing with other States. A structure to ensure accountability and transparency within governmental organizations carrying out surveillance needs to be clearly established in the law."

(ANNEXURE P-27, at Pg. 1047)

E. Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/27/37 (30 June 2014)

"*29. [S]ecret rules and secret interpretations – even secret judicial interpretations – of law do not have the necessary qualities of "law". Neither do laws or rules that give the executive authorities, such as security and intelligence services, excessive discretion. The secret nature of specific surveillance powers brings with it a greater risk of arbitrary exercise of discretion which, in turn, demands greater precision in the rule governing the exercise of discretion, and additional oversight. Several States also require that the legal framework be established*

through primary legislation debated in parliament rather than simply subsidiary regulations enacted by the executive – a requirement that helps to ensure that the legal framework is not only accessible to the public concerned after its adoption, but also during its development, in accordance with article 25 of the International Covenant on Civil and Political Rights."

(ANNEXURE P-27, at Pg. 1048)

F. Concluding Observations on the Fourth Periodic Report of the Republic of Korea, Human Rights Committee, U.N. Doc. CCPR/C/KOR/CO/4 (3 December 2015)

"*42. The Committee notes with concern that, under article 83 (3) of the Telecommunications Business Act, subscriber information may be requested without a warrant by any telecommunications operator for investigatory purposes. ...*

43. The State party should introduce the legal amendments necessary to ensure that any surveillance, including for the purposes of State security, is compatible with the Covenant. ***It should, inter alia, ensure that subscriber information may be issued with a warrant only.*****"**

(ANNEXURE P-27, at Pg. 1053)

G. U.N. General Assembly Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/RES/73/179 (17 December 2018)

"*6. Calls upon all States: (d) To establish or maintain existing* ***independent, effective, adequately resourced and impartial judicial, administrative and/or parliamentary domestic oversight mechanisms capable of ensuring transparency****, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data;*"

(ANNEXURE P-27, at Pg. 1056)

H. Concluding observations on the fifth periodic report of Belarus, Human Rights Committee, U.N. Doc. CCPR/C/BLR/CO/5 (22 November 2018

"*44. The State party should ensure that: ... (b) surveillance and interception is conducted subject to judicial authorization as well as effective and independent oversight mechanisms; ...*"

(ANNEXURE P-27, at Pg. 1056)

I. Report of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age, U.N. Doc. A/HRC/39/29 (3 August 2018)

"*39. Surveillance measures, including communications data requests to business enterprises and intelligence-sharing, should be authorized, reviewed and supervised by independent bodies at all stages, including when they are first ordered, while they are being carried out and after they have been terminated (see CCPR/C/FRA/CO/5, para. 5). The independent body authorizing particular surveillance measures,*

preferably a judicial authority, needs to make sure that there is clear evidence of a sufficient threat and that the surveillance proposed is targeted, strictly necessary and proportionate and authorize (or reject) ex ante the surveillance measures.

40. ***Oversight frameworks may integrate a combination of administrative, judicial and/or parliamentary oversight.*** *Oversight bodies should be independent of the authorities carrying out the surveillance and equipped with appropriate and adequate expertise, competencies and resources Authorization and oversight should be institutionally separated. Independent oversight bodies should proactively investigate and monitor the activities of those who conduct surveillance and have access to the products of surveillance, and carry out periodic reviews of surveillance capabilities and technological developments. The agencies carrying out surveillance should be required to provide all the information necessary for effective oversight upon request and regularly report to the oversight bodies, and they should be required to keep records of all surveillance measures taken. Oversight processes must also be transparent and subject to appropriate public scrutiny and the decisions of the oversight bodies must be subject to appeal or independent review. Exposing oversight bodies to divergent points of view, for example through expert and multi-stakeholder consultations (see for example A/HRC/34/60, para. 36), is particularly important in the absence of an adversarial process: it is essential that "points of friction" — continual challenges to approaches and understandings — be built in.*"

(ANNEXURE P-27, at Pg. 1056)

J. Report of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age, U.N. Doc. A/HRC/39/29 (3 August 2018)

"*41. State authorities and oversight bodies should also engage in public information about the existing laws, policies and practices in surveillance and communications interception and other forms of processing of personal data, open debate and scrutiny being essential to understanding the advantages and limitations of surveillance techniques (see A/HRC/13/37, para. 55). Those who have been the subject of surveillance should be notified and have explained to them ex post facto the interference with their right to privacy. They also should be entitled to alter and/or delete irrelevant personal information, provided that information is not needed any longer to carry out any current or pending investigation (see A/HRC/34/60, para. 38).*"

(ANNEXURE P-27, at Pg. 1061)

K. The Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, Freedom of Expression and the Internet (31 December 2013)

"*166. The State must be transparent with respect to the laws regulating communications surveillance and the criteria used for their application. The principle of "maximum disclosure" is applicable to this issue, and indeed governs all State acts: they are public and can only be kept secret from the public under the strictest circumstances, provided that this*

confidentiality is established by law, seeks to fulfil a legitimate aim under the American Convention, and is necessary in a democratic society.

167. As the European Court of Human Rights has held, ***a secret surveillance system can "undermine or even destroy democracy under the cloak of defending it****." The Court therefore demands that there be "adequate and effective guarantees against abuse." To determine whether this is being done in a particular case, the Court indicated that it is necessary to examine "nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorize, carry out and supervise them, and the kind of remedy provided by the national law*."

(ANNEXURE P-27, at Pg. 1061)

L. U.N. General Assembly Resolution on the safety of journalists and the issue of impunity, U.N. Doc. A/RES/72/175 (19 December 2017)

(On safety of Journalists)

"*Acknowledging also the particular risks with regard to the safety of journalists in the digital age, including the particular vulnerability of journalists to becoming targets of unlawful or arbitrary surveillance or interception of communications, in violation of their rights to privacy and to freedom of expression, ...*

"14. Emphasizes that, in the digital age, encryption and anonymity tools have become vital for many journalists to freely exercise their work and their enjoyment of human rights, in particular their rights to freedom of expression and to privacy , including to secure their communications and to protect the confidentiality of their sources, and calls upon States not to interfere with the use of such technologies and to ensure that any restrictions thereon comply with States' obligations under international human rights law;

(ANNEXURE P-27, at Pg. 1069)

6. **International Judgments**

A. Maximillian Schrems v. Data Protection Commissioner, C-362/14, Advocate General's Opinion, 23 September 2015

B. Maximillian Schrems v. Data Protection Commissioner, C-362/14, 6 October 2015

C. Big Brother Watch and Others v. the United Kingdom, No. 58170/03, communicated on 9 January 2014

D. CJEU, Joined Cases C-203/15 and C-698/15, Tele2 Sverige and Watson v. Home Secretary, 21 December 2016

E. ECHR, Roman Zakharov v. Russia [GC], No. 47143/06, 4 December 2015,

FACTUAL BACKGROUND

14. The present Writ Petition has been filed by the Petitioners in public interest under Article 32 of the Constitution of India seeking *inter alia* the issuance of the writ of Mandamus or any other appropriate order or direction, for bringing an end to the mass surveillance infrastructure being rolled out in the country with help of modern technology, bring India's communications surveillance infrastructure under judicial oversight, establishing a set of Guidelines by this Hon'ble Court and for an independent investigation into the use of specific malware in particular, the Pegasus spyware used for spying of Indian citizens including journalists, political opponents, judges and other persons.

15. Surveillance in India is undertaken within a regulatory framework outlined in The Indian Telegraph Act, 1885 and under the Information Technology Act, 2000 and the rules framed under the respective Acts. The Indian Telegraph Act, 1885 is a British-era legislation which was enacted to control and restrain telegraph communication during the colonial rule. The lack of safeguards

16. This is not the first time in history that our country is witnessing a misuse of surveillance being done by the government on its own citizens. In 1990, soon to be Prime Minister of India Shri Chandra Shekhar had publicly alleged that the V.P. Singh government was illegally tapping the telephone of a number of politicians and the list included him as well. This became a national scandal, followed by a CBI enquiry which revealed how illegal phone tapping was menacing our democracy. Since 2009, through newspaper reports we have been told about a number of

additional surveillance systems in varying stages of development that are currently in the works, including:

- The Centralized Monitoring System
- Network Traffic Analysis
- National Intelligence Grid

17. These systems are demonstrably among the most invasive in the world – all the more so, considering how a patchwork of broadly worded laws with questionable compliance rates allow them to tap into virtually any network, often without the knowledge of even service providers themselves. The aforesaid systems have been exempted from the purview of the RTI Act and the public has no information about their capabilities. Nor have these been tested against the tests laid down in the K.S. Puttaswamy judgment.

18. Surveillance systems such as CMS, NETRA and NATGRID seemingly conduct *perpetual mass surveillance*, affording no opportunities for cost-benefit-analyses in specific instances. It would appear that communications surveillance is mostly undertaken because it is the easiest available alternative, as opposed to the least intrusive. Petitioner No. 2 has been researching on the issue of India's surveillance since the 2013 Snowden revelations and has released research reports, created public awareness and conducted litigation to bring light to the lack of judicial or parliamentary oversight on India's surveillance infrastructure.

19. In 2013, the Indian Parliament was rocked once again by the issue of alleged surveillance of mobile phones of senior BJP leader Mr Arun Jaitley and all we saw was a direction by the Rajya Sabha committee on privileges, directing the Delhi Police to pursue a criminal case. An

application under the Right to Information Act filed by Petitioner No. 2 in 2014 revealed that on an average between 7,500 to 9000 orders for interception of telephones are issued by the Central Government alone, per month. On adding the surveillance orders issued by the State Governments to this, it becomes clear that India routinely conducts surveillance on her citizens' communications on a truly staggering scale.

20. An attack on Indian citizens using the Pegasus spyware was discovered in 2019 for the first time. The international press and the media in India had covered the issue extensively. It is during the first known attack on Indian citizens that Petitioner No. 1 was also targeted by the Pegasus spyware.

21. Despite being cornered by the press and by the members of parliament in 2019 and again in 2021, the central government refused to give a clear response on whether or not it had weaponised and used the Pegasus spyware against its own citizens. Since 2019, GoI has adopted an evasive stance and continues to operate in that mode without providing any clear answers on use of malware attacking its own citizens including journalists, activist, politicians and other innocent civilians. Instead of launching an investigation into the Pegasus issue, the government is continuously attempting to change the narrative and to suggest that the controversy had more to do with maligning India's democracy than its own contribution to the ongoing mess.

22. On March 11, 2020 GoI announced in Parliament, the full adoption of facial recognition technology enabled surveillance. In a parliamentary address, GoI announced that using photographic and other information from government "databases", 1,100 individual participants in the Delhi

riots had been identified. The number was later raised to 1,900. When other advanced democracies including the United States and European Union have been slowing down or stopping altogether uses of facial recognition in the public sphere, India seems to be travelling at top speed in the other direction.

23. Revelations in respect of an attack on Indian citizens, using the Pegasus spyware were made by The Wire in India, 19.07.2021 onwards. The NSO group has consistently maintained that it only sells spyware technologies to governments and state agencies. The legality of operations of such private surveillance companies is entirely questionable in view of the fact that the Information Technology Act expressly criminalizes the infiltration and discreet retrieval of information of the nature discussed above. The element of Government collusion only makes matters worse as LEAs seemingly have no qualms in skirting the law to procure desired information, leaving citizens constantly watching over their shoulder. Additionally, the discreet nature of these endeavours means there is no public accountability or oversight involved whatsoever. After the Pegasus revelation, every citizen is left to grapple with the rather unsettling question of what other discreet surveillance mechanisms are currently in deployment that we haven't had the fortune of coming to know of through chance encounters at security conferences.

24. Several provisions of law collectively enable the Government and its agencies to conduct communications surveillance on a variety of grounds with merely executive oversight and no involvement of the Judiciary or the Parliament. In addition to legislations, surveillance-enabling

clauses/conditions are also found across several communications service license agreements. Most surveillance-enabling laws and regulations rarely, if ever, see review in order to keep up with technological changes. For instance, provisions dealing with interception/monitoring of telephones are found under the archaic Indian Telegraph Act of 1885. Its provisions have also served as the bases for more recent additions such as Section 69 to the Information Technology Act, which was modelled after Section 5 of the Telegraph Act. In this particular instance, much of the language of law has been retained over the two Acts that are separated by over a century. So specific provisions contained in the enabling legislations do not reflect recent advancements in technology, leading to a significant amount of administrative difficulties to the detriment of all involved.

25. That the Petitioner No. 2 had earlier filed a Writ Petition bearing No. 8998 of 2020 before the Delhi High Court, as a Public Interest Litigation, praying for a stop to the operation of surveillance projects like NATGRID, CMS and NETRA rolled out by the Union Government and praying for the establishment of a permanent independent oversight body - judicial and/or parliamentary body, for issuing and reviewing interception and monitoring orders under the Telegraph Act, 1885 and the Information Technology Act, 2000. parliamentary/judicial oversight on . The said Petition was admitted before the Delhi High court on the same is pending adjudication before the same.

26. That the Petitioners submit that the acts of the respondents concerned are violative of the principles laid down in the Puttaswamy I (2017) and the PUCL Judgment.

27. In the backdrop of insurmountable evidence of the use of Pegasus spyware on Indian citizens, and the lack of any judicial oversight on such invasive surveillance measures, the Petitioners have been constrained to approach this Hon'ble Court by way of filing this writ petition, seeking a relief in an issue that is of nationwide significance.

28. The steps which have been initiated by the Respondents through various means and processes, have an eerie similarity with the dystopian world view as was depicted in George Orwell's 1984. The Respondents in this case are attempting to play the role of the all seeing big brother, keeping a watch on its citizens and their movements. If not stopped at the earliest, these processes have the potential to erode the rights of citizens and will cause irreversible and irreparable damage. At this point, careful consideration must be given to what B. R. Ambedkar said - "***If things go wrong under the new Constitution the reason will not be that we had a bad Constitution. What we will have to say is that Man was vile***".

29. That the facts constituting the cause of action are that there is that as a consequence of the faults in the surveillance framework in India and the misuse of the Pegasus spyware possibly by the Government authorities against their own citizens in India, there has been an erosion of the guarantees given under the Constitution of India, as a consequence of the violation of fundamental rights including the right to equality under Article 14, right to freedom of speech and expression under Article 19(1)(a), right to privacy as a subset of right to life under Article 21, and the right to freedom of trade under Article 19(1)(g) of the Constitution of India.

Given below is a chronological listing or the facts which are relevant to the present case:

(1990s)

30. In June, 1998, the Law Reform Commission of Ireland published a Report titled "Privacy: Surveillance and the Interception of Communications IRELAND (1997)" The Report by the Law Reform Commission on "*PRIVACY: Surveillance and the Interception of Communications*" consists of Ireland's Law Reform Commission's final recommendations with respect to privacy in the specific context of surveillance and the interception of communications. The Report also contains the privacy problem posed by surveillance in all contexts. A true copy of the Ireland Law Reform Commission report on "Privacy" Surveillance and the Interception of Communications" dated June, 1998 is marked and annexed hereto as **ANNEXURE P-1** ***(Pg. No 111 to 405)***

(2000s)

31. In May, 2005, the New South Wales Law Reform Commission of Australia, published its Report 108 titled "Surveillance: Final Report". The report was published in response to the Attorney General's direction to the commission to inquire and report on the scope and operation of the Listening Devices Act, 1984 and the need to regulate the use of visual surveillance equipment and any related matters thereto. A true copy of the Report by the New South Wales Law Reform Commission of

Australia titled "Surveillance: Final Report" dated May, 2005 is marked and annexed hereto as **ANNEXURE P-2** ***(Pg. No 406 to 517)***.

(2009)

32. In the aftermath of the 26/11 attacks in Mumbai, the Federation of Indian Chamber of Commerce (FICCI) published a report titled " *FICCI Task Force Report on National Security & Terrorism (Volume 1).*" The Report was prepared under the Chairmanship of Mr. Rajeev Chandrasekhar and it was presented to Home Minister Mr. P. Chidambaram in November, 2009. The Report contained a broad vision and a set of recommendations on counter-terrorism measures for the consideration of the Central Government. One of the recommendations given in the Report was for the development of a "National Intelligence Grid." Following is a relevant extract from the Report on the aforementioned recommendation: "*To create a national information exchange grid, gathering data from varied sources such as telecom, banking, immigration, national identities, electronic spectrum, and existing intelligence, police, paramilitary and other government agencies and funnel it through powerful analytics capability to predict trends, events and create 'over the horizon' visibility within the next 24-36 months. This grid will have strong analytics and pattern recognition capabilities to decipher relationships between seemingly unrelated events.*" (Pg. 14 of the Report).

(2012)

33. On 16.10.2012, the Group of Experts on Privacy constituted by the Planning Commission under the chairmanship of Justice Ajit Prakash Shah published its Report. The report contains international privacy principles, national privacy principles, rationale and emerging issues along with an analysis of legislations/Bills from a privacy perspective. On the lack of Judicial Oversight, the committee states the following:

> "***The regime does not require judicial oversight or authorization***, *it is unclear which agencies are legally authorized to undertake interception/access, systematic access or proactive disclosure of communications and classes of data is not prohibited, agencies are not required to be transparent to the public regarding the effectiveness and cost of each intercept, interception/access is permitted for even minor offenses, there is no requirement for standardization of orders, there are no additional safeguards for when interceptions/access invade individual's privacy beyond the targeted subject, and the individual is never notified that an interception/access took place, even after the close of the investigation.*" (emphasis supplied)

A true copy of the relevant portions of the Report by the Group of Experts on Privacy, dated 16.10.2012 is marked and annexed hereto as **ANNEXURE P-3** ***(Pg. No 518 to 538)***

(2013)

34. **Snowden Revelations**

Edward Snowden, a former contractor with the Central Intelligence Agency (CIA) in the United States, leaked details about the extensive internet and phone surveillance that American Intelligence was involved in. The US National Security Agency tapped directly into the servers of 9 internet firms including Facebook, Google, Microsoft and Yahoo, to track online communication in a surveillance project called PRISM.

35. **Necessity and Proportionate Principles**

In 2013, a set of principles was drafted by a coalition of civil society, privacy and technology experts. The set of principles have been endorsed by more than 600 organizations and over 2,70,000 individuals around the world. A true copy of the International Principles on the Application of Human Rights to Communications Surveillance (the "Necessary and Proportionate Principles" or "13 Principles"), dated 2013, is marked and annexed hereto as **ANNEXURE P-4** ***(Pg. No. 539 to 553)***

Citizen Lab Reports

36. Citizen Lab is a digital surveillance research agency based out of Toronto, Canada. It is based at the Munk School of Global Affairs & Public Policy, University of Toronto. On15.01.2013, Citizen Lab published a report titled ""*Planet Blue Coat Mapping Global Censorship and Surveillance Tools*",

37. "*Planet Blue Coat Mapping Global Censorship and Surveillance Tools*", elaborates upon a company called Blue Coat Systems which is a

California based provider of network security and optimization products. In its "Key Findings" section, the Report states:

> "***Blue Coat Devices capable of filtering, censorship, and surveillance are being used around the world***. *During several weeks of scanning and validation that ended in January 2013, we uncovered 61 Blue Coat ProxySG devices and 316 Blue Coat PacketShaper appliances, devices with specific functionality permitting filtering, censorship, and surveillance.* ***61 of these Blue Coat appliances are on public or government networks in countries with a history of concerns over human rights, surveillance, and censorship*** *(11 ProxySG and 50 PacketShaper appliances). We found these appliances in the following locations: Blue Coat ProxySG: Egypt, Kuwait, Qatar, Saudi Arabia, the UAE. PacketShaper: Afghanistan, Bahrain, China,* ***India****, Indonesia, Iraq, Kenya, Kuwait, Lebanon, Malaysia, Nigeria, Qatar, Russia, Saudi Arabia, South Korea, Singapore, Thailand, Turkey, and Venezuela.*" (emphasis supplied)

The report further talks about the software "PacketShaper" in the following words:

> "*PacketShaper, a cloud-based network management device that* ***can establish visibility of over 600 web applications and control undesirable traffic****. ProxySG provides "SSL Inspection" services to solve "...issues with intercepting SSL for your end-users."* ***PacketShaper is integrated with WebPulse, Blue Coat Systems' real-time network intelligence service that can filter application traffic by content category.*** *Blue Coat Systems states that it*

"provides products to more than 15,000 customers worldwide," and indeed, it maintains offices globally, including in Latin America, the Middle East, and the Asia Pacific region." (emphasis supplied)

The report mentions that the presence of PacketShaper installations were found in a number of countries including India. In this context It states:

"*We discovered PacketShaper installations in the following countries of interest: Afghanistan, Bahrain, China,* ***India,*** *Indonesia, Iraq, Kenya, Kuwait, Lebanon, Malaysia, Nigeria, Qatar, Russia, Saudi Arabia, South Korea, Singapore, Thailand, Turkey, and Venezuela. We were able to visit these hosts and confirm that they were running the product.....*" (emphasis supplied)

A true copy of the report published by Citizen Lab titled "*Planet Blue Coat, Mapping Global Censorship and Surveillance Tools*" dated 15.01.2013 is marked and annexed hereto as **ANNEXURE P-5** ***(Pg. No. 554 to 584)***.

38. According to another report by Citizen Lab dated 13.03.2013 and titled "*For Their Eyes Only: The Commercialization of Digital Spying.*", a surveillance software called **FinFisher** which was created by a Munich based company Gamma International GmbH, has been found on servers in India. This technology has been used to target human rights activists and opposition leaders in other countries. The report contains a description of the results obtained after a comprehensive global internet scan for command and control servers of FinFisher surveillance

software. The report gives a description of FinFisher in the following words:

> "***FinFisher is a line of remote intrusion and surveillance software developed by Munich-based Gamma International GmbH. FinFisher products are marketed and sold exclusively to law enforcement and intelligence agencies by the UK-based Gamma Group***. *Although touted as a "lawful interception" suite for monitoring criminals, FinFisher has gained notoriety because it has been used in targeted attacks against human rights campaigners and opposition activists in countries with questionable human rights records*." (emphasis supplied)

The report in its "Summary of Key Findings" section states:

> "*We have found command and control servers for FinSpy backdoors, part of Gamma International's FinFisher "remote monitoring solution," in a total of 25 countries: Australia, Bahrain, Bangladesh, Brunei, Canada, Czech Republic, Estonia, Ethiopia, Germany,* ***India****, Indonesia, Japan, Latvia, Malaysia, Mexico, Mongolia, Netherlands, Qatar, Serbia, Singapore, Turkmenistan, United Arab Emirates, United Kingdom, United States, Vietnam.*" (emphasis supplied)

A true copy of the relevant extracts of the report published by The Citizen Lab titled "*For Their Eyes Only: The Commercialization of Digital Spying*" dated 01.05.2013 is marked and annexed hereto as **ANNEXURE P-6 (pages 585 to 617)**.

39. On 17.04.2013, the United Nations General Assembly published the "*Report of the Special Rapporteur on the promotion and protection of*

the right to freedom of opinion and expression, Frank La Rue". The report analyses the implications of States' surveillance of communication on the exercise of the right to privacy and the right to freedom of opinion and expression. The report states: "*In many States, communication service providers are being compelled to modify their infrastructure to enable direct surveillance, eliminating the opportunity for judicial oversight. For example, in 2012 the Colombian Ministries of Justice, and Information and Communication Technologies, issued a decree that required telecommunication service providers to put in place infrastructure allowing direct access to communications by judicial police, without an order from the Attorney General. The above-mentioned Uganda's Regulation of Interception of Communications Act 2010 (s3) provides for the establishment of a monitoring centre and mandates that telecommunications providers ensure that intercepted communications are transmitted to the monitoring centre (s8(1)(f)). The Government of India is proposing to install a Centralized Monitoring System that will route all communications to the central Government, allowing security agencies to bypass interaction with the service provider. Such arrangements take communications surveillance out of the realm of judicial authorization and allow unregulated, secret surveillance, eliminating any transparency or accountability on the part of the State.*" A true copy of the UNGA Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression dated 17.04.2013 is marked and annexed hereto as **ANNEXURE P-7 *(Pg. No. 618 to 640)***.

40. On 11.06.2013, The Guardian published a news article titled "*Boundless Informant: the NSA's secret tool to track global surveillance data*." The article contains information obtained from secret documents about the NSA data-mining tool called "Boundless Informant" which in a country wise manner, details and maps the volume of information it had collected from computer and telephone networks. The article states that as per the top secret NSA "global heat map" which was seen by the Guardian, Iran was the country from where the largest amount of intelligence was gathered, and India was at the fifth position. A true copy of The Guardian article titled "*Boundless Informant: the NSA's secret tool to track global surveillance data*" dated 11.06.2013 is marked and annexed hereto as **ANNEXURE P-8** ***(Pg. 641 to 644)***

41. **Implementation of CMS and Amendment of Unified License Agreement**

On 11.10.2013, the Central Government vide Amendment 2 of 2013, amended the Unified License Agreement, in order to implement the Central Monitoring System. As per the amended terms of the License, the Licensee's Lawful Interception System needs to be connected to the CMS at Regional Monitoring Center at Regional Monitoring Center (RMC), through interception Store and Forward (ISF) server placed in the Licensee's premises. A true copy of the Unified License Agreement Amendment 2 of 2013 dated 11.10.2013 and the License Agreement for Unified Access Services (UAS) is marked and annexed hereto as **ANNEXURE P-9 (COLLY)** ***(Pg. 645 to 732)***.

42. The license agreements currently governing provision of fixed-line/mobile telephone and internet services, namely: Unified Access Service License (UASL), Internet Service License (ISL), Unified License (UL). All of the above-mentioned license agreements require their licensees to furnish 'all necessary means and facilities as required' for the application of Section 51 of the Indian Telegraph Act. Licensees must also provide in the interests of security, 'suitable monitoring equipment' as per the requirement of the DOT or LEAs. The specific orders or directions from the Government issued under such conditions (i.e. in the interests of security) are also applicable. Further, licensees are obliged to provide all tracing facilities to trace nuisance and obnoxious/malicious communications passing through their networks, when such information is required for investigations or detection of crimes, and in the interest of national security. They must also provide 'necessary facilities' depending upon the specific situation at the relevant time, to counteract espionage, subversive act, sabotage or any other unlawful activity. Both the UASL and the UL require their licensees to archive all commercial records/Call Data Records/Exchange Data Records/IP Data Records with regards to communications exchanged in their networks for a period of one year for security reasons.

(2014)

43. In January 2014, the Civil Liberties (LIBE) Committee of the European Parliament voted to invite Edward Snowden to testify to its inquiry on electronic mass surveillance. In his testimony, Snowden talks about the surveillance program by the NSA, the value of an oversight mechanism

and the risks associated with Surveillance. A true copy of the testimony given by Edward Snowden before the LIBE Committee, dated January, 2014 is marked and annexed hereto as **ANNEXURE P-10** ***(Pg. No. 733 to 744)***.

44. On 08.01.2014, Petitioner No. 2 received a reply to an RTI which was filed seeking information on a Delhi Police tender, inviting technology companies to supply internet monitoring equipment. In 2011, the Provisioning & Logistics Department of the Delhi Police had issued a global notice inviting "expression of interest" from Indian and foreign technology companies to supply Internet monitoring equipment. Petitioner No. 2 then filed an RTI application before the Delhi Police in December 2013, seeking a list of companies that had responded to this notice. The response to the RTI revealed 26 Indian and foreign companies as having expressed interest in supplying monitoring equipment. A true copy of the RTI Reply sent by the Delhi Police, dated 08.01.2014 is marked and annexed hereto as **ANNEXURE P-11** ***(Pg. No. 745 to 747)***.

45. In 2014, Petitioner No. 2 published a report titled "*India's Surveillance State*". The report details several aspects of communication surveillance in India and takes an in-depth look at India's surveillance machinery, including the enabling provisions of law, service provider obligations and known mechanisms. A true copy of the report published by Petitioner No. 2 titled "*India's Surveillance State*" dated 2014 is marked and annexed hereto as **ANNEXURE P-12** ***(Pg. No 748 to 815)***

46. On 11.02.2014, In response to a question asked before the Lok Sabha on reports of illegal phone tapping, the then Minister of State in the Ministry of Home Affairs Shri R.P.N. Singh acknowledged the incidents of physical/electronic surveillance which had been conducted without authorization. Following is an extract taken from his response:

> "*Incidents of physical/electronic surveillance in the States of Gujarat and Himachal Pradesh, and the National Capital Territory of Delhi, allegedly without authorization have been reported. Union Cabinet has approved a proposal to set up a Commission of Inquiry under Commission of Inquiry Act, 1952 to look into these incidents.*"

A true copy of the Lok Sabha starred Question No. 294 along with the response dated 11.02.2014 is marked and annexed hereto as **ANNEXURE P-13** ***(Pg. No 816 to 818)***

47. In March 2014, Maria Xynou, a researcher with the Center for Internet and Society, India, authored a report titled "*The Surveillance Industry in India.*" The report contains the findings of the research conducted by The Center for Internet and Society (CIS) to investigate the growth of the surveillance industry in India, specifically in the aftermath of the 2008 Mumbai terrorist attacks. The report contains some startling revelations about the sale of surveillance technologies by private companies. E.g. the report mentions ClearTrail Technologies which is an Indian company based in Indore. Describing the capabilities of ClearTrail, the report states: "*The document titled "Internet Monitoring Suite" from ClearTrail Technologies illustrates the company's mass monitoring, deep packet*

inspection, COMINT, SIGINT, tactical Internet monitoring, network recording and lawful interception technologies." The report contains details in respect of a number of other such companies and the surveillance technologies being developed or sold by them. A true copy of the Report titled "*The Surveillance Industry in India*" by Maria Xynou, dated March, 2014 is marked and annexed hereto as **ANNEXURE P-14** ***(Pg. No 819 to 866)***

48. On 12.05.2014, Petitioner No. 2 received an RTI reply from the CPIO, Ministry of Home Affairs, stating that around 7500-9000 orders for interception of telephones are issued by the Central Government per month. A true copy of the RTI response received by the 2nd Petitioner on 12.05.2014 is marked and annexed hereto as **ANNEXURE P-15** ***(Pg. 867)***

(2015)

49. **Number of Interception Orders issued monthly - Response in Lok Sabha**

In response to a Lok Sabha Question regarding the number of phones which are tapped every month in India, on 04.03.2015, the then Minister of Communications and Information Technology Shri Ravi Shankar Prasad gave the following response: "*Madam, on an average 5000 interception orders per month are issued by the Union Home Secretary on the requests supported by justified grounds/ reasons made by Law Enforcement Agencies*." It is pertinent to mention that this figure highlights the inherent fallacy in the authorization mechanism for communication surveillance in India. The Secretary in the Ministry of

Home Affairs in the Central Government has the responsibility for authorizing requests for the interception, monitoring, and decryption of communications issued by Central agencies, and the Secretary in charge of the home department is responsible for authorizing requests for the interception, monitoring and decryption of communications from state level agencies and law enforcement. It is questionable as to how the union home secretary in this case would be able to peruse, apply his/her mind and then make a sound decision in respect of so many Orders, given the fact that he/she also shoulders many other responsibilities. The proportionality test encapsulates within itself the element of necessity which means that interception of communication should only be done when it is the least restrictive way of achieving a legitimate purpose. It is not very clear if that principle is being applied when a total of 5000 Orders are being issued per month. A true copy of the Lok Sabha Unstarred Question No. 1443 along with the response, dated 04.03.2015 is marked and annexed hereto as **ANNEXURE P-16** ***(Pg. 868 to 869)***

50. **On the Nexus between Government and Private surveillance Technology Companies**

On 10.07.2015, NDTV published a news article titled "*UPA Was Client of Controversial Italian Spyware Firm, Claim Leaked Mails.*" The article points to a nexus between the Central Government and companies that sold software which was used for spying. In this context, the article states: "*But the leaked emails seem to suggest demos for a wider use of collecting information from cellphones - an email from last month talks*

of the Andhra Pradesh Police looking for this sort of software". The article further states: "*Emails in 2010 reveal the Indian embassy in Italy asking Hacking execs to present demos in Delhi to the government about "the remote control system V6 spyware.*" A true copy of the Article published by NDTV titled "*UPA Was Client of Controversial Italian Spyware Firm, Claim Leaked Mails*" dated 10.07.2015 is marked and annexed hereto as **ANNEXURE P-17** ***(Pg. No 870 to 871).***

51. On 15.07.2015, The Economic Times published a news article titled "*Why Indian Intelligence uses small companies like Sunworks Consultants for spying technology*". The article elaborates upon a nexus between Indian Intelligence agencies and private entities, in the backdrop of obtaining surveillance technologies. The article states:

> "*There's nothing remotely James Bond-like about the drab corner in Gurgaon. But then, what better cover for a spot of cloak-and-dagger activity? Perhaps, for this is the home of Sunworks Consultants, which says it provides IT services to the healthcare and telecom space.* ***But in a series of emails to Italian spyware firm Hacking Team, the company negotiated for high-end surveillance equipment that it said it was buying for the Research & Analysis Wing, India's intelligence agency. In emails released by Wikileaks last week, Sunworks even said the licences had to be in its name because RAW cannot buy from foreign agencies. ET sifted through more than 3,400 Hacking Team emails, which reveal that India's security services are buying spying technology, mostly through little known outfits that act as go-betweens***."

A true copy of the article published by The Economic Times titled "*Why Indian Intelligence uses small companies like Sunworks Consultants for spying technology*", dated 15.07.2015 is marked and annexed hereto as **ANNEXURE P-18** ***(Pg.872 to 874)***

52. **On instances of Illegal Phone Tapping in India**

On 12.08.2015, in response to a Rajya Sabha question on instances of illegal phone tapping, the then Minister of State in the Ministry of Home Affairs Shri Haribhai Paratibhai Chaudhary gave the following response:

> "*Recently, a few cases have been registered in different Police Stations in Andhra Pradesh relating to allegations of illegal phone tapping. All these cases are under investigation at present.*"

A true copy of the Rajya Sabha Unstarred Question No. 2593, along with the response dated 12.08.2015, is marked and annexed hereto as **ANNEXURE P-19** ***(Pg. 875 to 876)*** It would be relevant to draw a reference to the NDTV article mentioned in Para 22 of this Additional Affidavit and the peculiar set of facts mentioned therein. The article discusses the contents of leaked emails which suggest that Andhra Pradesh police was looking for surveillance software. Although there exists no evidence to link to two separate set of circumstances, the coincidence evokes curiosity and merits an investigation.

53. On 18.11.2015, the European Union Agency for Fundamental Rights (FRA) published its Report on "Surveillance by intelligence services - Volume I: Member States' legal frameworks" In response to the Snowden revelations, the European Parliament had passed a resolution

which among others, asked the European Union Agency for Fundamental Rights to undertake a research on the fundamental rights protection in the context of surveillance and the available remedies. The Report gives an overview of the legal framework of the EU member states in respect of surveillance. A true copy of the report published by the European Union Agency for Fundamental Rights (FRA) titled "Surveillance by intelligence services - Volume I: Member States' legal frameworks", dated 18.11.2015 is marked and annexed hereto as **ANNEXURE P-20** ***(Pg. No. 877 to 976)***

54. On 15.12.2015, the Venice Commission published its Report on the Democratic Oversight of Signals Intelligence Agencies. The Report was Adopted by the Venice Commission at its 102nd Plenary Session (Venice, 20-21 March 2015) The report explores the impact of signals intelligence on privacy, among other aspects. A true copy of the Venice Commission report on Democratic Oversight of Signals Intelligence Agencies dated 15.12.2015 is marked and annexed hereto as **ANNEXURE P-21** ***(Pg. No 977 to 1014)***

(2016)

55. **Reports of Snooping on the public by the Government**

On 07.06.2016, The Hindu published/updated a news article titled "*India gets ready to roll out cyber snooping agency*". The article talks about the setting up of the National Cyber coordination Center (NCCC) and talks about the monitoring of internet (traffic) by the government.

On this point, the article states: "*Though the government won't say that they would be able to look into your Facebook or Twitter accounts as and when required, the fact remains that the setting up of the federal Internet scanning agency will give law enforcement agencies direct access to all Internet accounts, be it your e-mails, blogs or social networking data.' The NCCC will collect, integrate and scan [Internet] traffic data from different gateway routers of major ISPs at a centralised location for analysis, international gateway traffic and domestic traffic will be aggregated separately ... The NCCC will facilitate real-time assessment of cyber security threats in the country and generate actionable reports/alerts for proactive actions by the concerned agencies," says a secret government note.*" A true copy of the The Hindu news article titled "*India gets ready to roll out cyber snooping"* dated 07.06.2016 is marked and annexed hereto as **ANNEXURE P-22** ***(Pg 1015 to 1016).***

56. On 21.08.2016, The Hindu published/updated an article titled "*Govt. violates privacy safeguards to secretly monitor Internet traffic*". The article contains the findings of an investigation which was undertaken by The Hindu, revealing that the internet activity of India's users was being subjected to wide ranging surveillance and monitoring and that much of this surveillance was in violation of the applicable rules and notifications for ensuring privacy of communications. A true copy of the news article published by The Hindu titled "*Govt. violates privacy safeguards to secretly monitor Internet traffic"*, dated 21.08.2016 is marked and annexed hereto as **ANNEXURE P-23** ***(Pg. 1017 to 1019)***

(2017)

57. **Inter-ministerial panel criticizes NTRO's engagement with a private company for snooping technology**

On 09.03.2012, The Hindu Businessline published/updated an article titled "*Panel slams roping in of private firm for Net snooping*". The article points out that an inter-ministerial panel slammed the National Technical Research Organization (NTRO) for "*roping in a private company or setting the Internet monitoring system*". The article further states that the committee also raised serious security concerns on the tie up as "*the private company was selling similar solutions to other customers in the global market, thus not exclusive to India*". The article highlights the dangerous trend of participation of private players in building up the surveillance infrastructure in the country and highlights the dangers that come with such partnerships. A true copy of the news article published by The Hindu Businessline article titled "*Panel slams roping in of private firm for Net snooping*" dated 09.03.2012, updated on 14.11.2017 is marked and annexed hereto as **ANNEXURE P-24** ***(Pg. 1020 to 1022)***

(2018)

58. **Sri Krishna Committee Report**

On 27.07.2018, the Justice BN Srikrishna Committee submitted its report titled "*A Free and Fair Digital Economy, Protecting Privacy, Empowering Indians*" to the Union Minister for Electronics and IT, law and Justice Shri Ravi Shankar Prasad. In the context of intelligence

gathering, the report on page 124 states: "*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.*** *There is no general law in India today that authorises non-consensual access to personal data or interception of personal communication for the purposes of intelligence gathering or national security. If there are any entities that are carrying out activities of such a nature without statutory authorisation (for example, solely through executive authorisation), such activities would be illegal as per the Puttaswamy judgment as they would not be operating under law. The Intelligence Services (Powers and Regulation) Bill, 2011 had been introduced to regulate the manner of functioning of Indian intelligence agencies and institute an oversight mechanism. However, the Bill lapsed in 2011 and left the legislative vacuum unaddressed."*

Discussing the oversight mechanism of monitoring and interception, the Report on page 125 states: "*For each of these mechanisms, oversight is carried out through a Review Committee set up under the Telegraph Rules. This Committee reviews interception orders passed under the Telegraph Act and Section 69B of the IT Act. It consists of the Cabinet Secretary, Secretary to the Government of India in charge of Legal Affairs and the Secretary to the Government of India in charge of*

Department of Telecommunications. As per a recent RTI application to the Ministry of Home Affairs, it has been found that about 7500-9000 such orders are passed by the Central Government every month. Highlighting the shortcoming and the insufficiency within the existing oversight mechanism, the Report further states: "*The Review Committee has an unrealistic task of reviewing 15000-18000 interception orders in every meeting, while meeting once in two months."* A true copy of the relevant parts of the BN Srikrishna Committee Report dated July, 2018 is marked and annexed hereto as **ANNEXURE P-25 *(Pg. 1023 to 1030).***

(2019)

59. On 15.02.2019, as a part of its ongoing efforts in research and advocacy on surveillance and its impact on constitutional rights in India, Petitioner No. 2 sent its submissions titled “Submission: The Surveillance Industry and Human Rights” to Mr. David Kaye, who was at the time, the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. A true copy of the submissions sent to the UN Special Rapporteur by Petitioner No. 2, dated 15.02.2019 is marked and annexed hereto as **ANNEXURE P- 26 *(Pg. No. 1031 to 1038)***

60. Privacy international is a United Kingdom based charity organization that has been working to promote human right of privacy throughout the world since 1990. On 28.02.2019, Privacy International published a guide document titled “Guide to International Law and Surveillance 2.0”. The guide contains a comprehensive collation of all the information collected from significant judgments and international legal instruments from around the world. The guide document covers topics such as the

illegality of mass surveillance operations, the law on data retention, extraterritorial application of human rights law and digital surveillance. A true copy of the guide document published by Privacy International titled "Guide to International Law and Surveillance 2.0", dated 28.02.2019 is marked and annexed hereto as **ANNEXURE P-27** ***(Pg. No 1039 to 1192)***.

61. **Report of the UN Special Rapporteur on Surveillance and Human rights**

On 28.05.2019, the UN Special Rapporteur presented a report on the adverse effect of the surveillance industry on freedom of expression (A/HRC/41/35) to the United Nations Human Rights Council. The report talks about targeted surveillance and the regulation of public-private collaboration in the sale, transfer, use and after-sales support of surveillance technologies. Some of the key recommendations in the report include: to establish a moratorium on the global sale and transfer of private surveillance technology till the time human rights safeguards are put in place to regulate such practices; States purchasing surveillance technologies should take measures to ensure that their use is in compliance with international human rights law. Petitioner No. 2 had also sent its submission in furtherance of seeking inputs/contributions from civil society members on this issue. A true copy of the UN Special Rapporteur's report on the promotion and protection of the right to freedom of opinion and expression: Surveillance and human rights, dated 28.05.2019, is marked and annexed hereto as **ANNEXURE P-28** ***(Pg. No. 1193 to 1213)***.

62. **Instances of Snooping on Indians**

In 2019, Indian citizens had reportedly fallen victim to the Pegasus spyware. Pegasus was used to hack into the mobile devices of 121 Indian citizens, including lawyers and human rights activists. Petitioner No. 1 was presumably attacked by the Pegasus spyware in the year 2019. On 29.10.2019 he received a message from WhatsApp pointing out a vulnerability, stating as follows: "*In May we stopped an attack where an advanced cyber actor exploited our video calling to install malware on user devices. There is a possibility this number was impacted, and we want to make sure you know how to keep your mobile phone secure"*. A true copy of the screenshot containing a message from WhatsApp to Petitioner No. 1, dated 29.10.2019 is marked and annexed hereto as **ANNEXURE P-29** ***(Pg. 1214).***

63. On 29.10.2019, Petitioner No. 1 was contacted by Citizen Lab, informing him and warning him against a specific cyber risk that their research indicated he had faced.

Statement by Former Home Secretary on the NSO Group

64. On 01.11.2019, The Quint published an article titled "*Govt Knew NSO, Other Spyware Firms Operated in India: Ex-Home Secy*" The article quotes former home secretary GK Pillai as saying that he was aware that Israeli Tech firm NSO had been operating in India and that it had sold spying software to private firms and individuals in the country. The article states:

"*Former home secretary GK Pillai told The Quint on Friday, 1 November, that he is aware that Israeli tech firm NSO had been operating in India – and that it had sold spying software to private firms and individuals in the country. He also confirmed that Indian government agencies have bought spyware in the past from private foreign tech firms like NSO. In fact, he said, "it is quite common."*

A true copy of the article published by The Quint titled "*Govt Knew NSO, Other Spyware Firms Operated in India: Ex-Home Secy* ", dated 01.11.2019 is marked and annexed hereto as **ANNEXURE P-30** ***(Pg. 1215 to 1218).***

65. **Letter to the Standing Committee on Information Technology**

On 19.11.2019, Petitioner No. 1 along with 16 other civil society activists and human rights defenders who had been targeted by the NSO-Pegasus Spyware, wrote a letter to the Parliamentary Committee on Information Technology, detailing the factual situation in the following words:

"*Today, we wish to bring to your notice one other circumstance that unites us. Over the last month, we have all received official communication from WhatsApp and Citizen Lab informing us that our mobile devices have been targets of highly sophisticated cyber-attacks. According to this official communication, spyware has been implanted in our mobile devices through WhatsApp's video calling service. This compromises our digital security and makes it possible for the attacker to gain access to and tamper with the functioning of*

our mobile devices and as a result, all other electronic devices to which they are linked."

The letter further requested the Committee to take action. Following is an extract from the letter containing the requests:

"*In view of the above, we request the committee to take two actions. First, at present, some of us are willing and forthcoming to provide oral testimony to the Standing Committee. We request you to kindly consider this. Second, we urge the Members of the Standing Committee to summon relevant government departments to place the following questions with a view towards gaining greater factual accuracy around this grave injury to our personal privacy and digital security.*

1. Which agencies and entities are carrying out this targeted and unauthorised surveillance of Indian citizens?

2. Are sections of the Indian government, central or state, involved in deployment of the Pegasus software?

3. Has public money been expended for these illegal and unauthorised attacks? Who authorised this expenditure?

4. Are central security agencies aware of the presence of NSO Group employees and operatives in India? Have these operatives entered the country legally?

5. Who were the individuals under surveillance by the Central or State agencies using this or other related technology?

6. What steps is the government taking to identify and bring to book the entities involved in the Pegasus attacks and other possible

instances of illegal and unauthorised surveillance of Indian citizens?

7. What steps is the government taking to identify and repair the breaches in the national telecommunications infrastructure and protect it against any further attacks?

8. In the interests of transparent, accountable and responsive governance, we urge you to also make public the details of the companies, agencies and other entities authorised by the Government of India to carry out surveillance in accordance with legal provisions. What are the terms and conditions that govern the operations of these agencies? What are the arrangements for monitoring and overseeing their work?"

A true copy of the letter sent by Petitioner No. 1 along with 16 other Civil Society activists and human rights defenders to the Parliamentary Committee on Information Technology, dated 19.11.2019 is marked and annexed as **ANNEXURE P-31** ***(Pg. No 1219 to 1222).***

(2020)

66. On 25.02. 2021 The Ministry of Electronics and Information Technology (*hereinafter* "MeitY") and the Ministry of Information and Broadcasting (*hereinafter "*MIB*"*) notified the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (*hereinafter* "Rules, 2021"). The Intermediary Guidelines replace the Information Technology (Intermediaries Guidelines) Rules, 2011 (*hereinafter, "*Rules 2011*"*). Amongst various other controversial provisions, one of the provisions is the "traceability or the originator" provision. It requires

significant social media intermediaries, which is a new class created under the 2021 Rules, to trace the first originator of a message. This provision would be applicable on tech companies like Facebook, Signal, WhatsApp, Telegram, Instagram. Traceability means that companies will have to compromise on End-to-End ('E2E') encryption. In this regard, E2E encryption means that messages between two individuals cannot be accessed by any other entity including the social media intermediary. Therefore, any compromise on the E2E encryption design undermines the hitherto-existing privacy of communication over messaging apps, as ensured through end-to-end encryption.

(2021)

The Pegasus Attack in India: Part II

67. On 19.07.2021, news media house The Wire published a series of reports, containing startling revelations about the use of Pegasus on a number of Indian Citizens.

About Pegasus

68. Pegasus is a surveillance software or a spyware which is used to spy on individuals by infiltrating their mobile devices. The spyware uses a dehumanizing and invasive technique on unsuspecting victims. Once it enters a mobile device, it has the potential to discreetly transfer various kinds of data on the device such as text messages, images, call data.

How Does Pegasus Operate

69. After the spyware is installed on a mobile device, it starts getting in touch with the operator. Once it is installed on a mobile device, it has the potential to discreetly send private data available on the mobile device

which includes text messages, event schedules, contacts, passwords, voice calls on messaging apps, location data etc. All of this is done without the knowledge or the permission of the user. The spyware also has the potential to turn on the phone camera and microphone, and spy on an individual's calls and activities. After the malware is installed on the phone, it can even use some bypassing methods and read encrypted messages which are exchanged on text messaging applications such as WhatsApp, Telegram etc.

70. One of the distinguishing features of the spyware which also makes it very popular, is the "Zero click attacks" feature. Zero-Click attack means that the victim is not required to click on a link or open an attachment for his device to be infected with the spyware.

Lack of clarity in the Responses given by the government

71. Following is a table indicating the response given by the Central Government on the Pegasus issue, at various points in time:

Sr. No.	Date	Name and Designation	Statement given
1.	19.07.2021	Shri Ashwini Vaishnav, Minister for Communications, Electronics & Information	dismissed reports about the use of Pegasus for spying on journalists, activists and opposition leaders. He said without a technical analysis, it was not possible to say whether or not there had been an attempted hack. He further gave

		Technology and Railways,	the following statement on the floor of the Parliament: "*In India there is a well-established procedure through which lawful interception of electronic communication is carried out in order for the purpose of national security, particularly on the occurrence of any public emergency or in the interest of public safety, by agencies at the Centre and States," the government added. "The requests for these lawful interceptions of electronic communication are made as per relevant rules under the provisions of section 5(2) of Indian Telegraph Act ,1885 and section 69 of the Information Technology (Amendment) Act, 2000.*"
2.	11.12.2019	Shri Anumula Revanth Reddy, Minister for	"*Government had been informed by WhatsApp of a vulnerability affecting some WhatsApp mobile users' devices*

		Electronics & Information Technology	*through a spyware namely Pegasus. 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. Some statements have appeared based on reports in media, regarding breach of privacy of Indian citizens on WhatsApp. 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"
3.	28.11.2019	Shri Ravi Shankar Prasad, Minister for Electronics and Information Technology and Communications	When asked whether the Government of India had sought the services of Pegasus malware, the Minister said: "*no unauthorized interception has been done, to the best of my knowledge"*. When asked whether there had been any transaction between the Indian Government and the NSO, the minister said: " *I have very specifically stated that the security agencies responsible follow a particular procedure. If there is any violation of particular procedure, we take action, tough action and also impose penalty*". Despite repeated questions on the issue, the minister failed to give a clear answer, affirming or denying the existence of a transaction or a deal between the Indian government and NSO
4.	20.11.2019	Shri Ravi	In response to a question asked in

		Shankar Prasad, Minister for Electronics and Information Technology and Communications	the Lok Sabha by Shri Asaduddin Owaisi on the Pegasus attack and the alleged use and purchase of the Pegasus spyware by Government agencies, the Minister of Electronics and Information Technology Shri Ravi Shankar Prasad gave the following response: *"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*."

It is therefore evident from all the responses given by the Central government that despite being asked repeatedly, it has failed to clear the air on the following questions:

i. Was there an **arrangement** between the central government and/or any of its agencies with the **NSO Group** for the purchase/supply of the Pegasus spyware?

ii. Has the central government or any of its agencies used the **Pegasus software** to spy on its **citizens**?

iii. If the government claims that it hasn't used Pegasus on its citizens, has it launched an **investigation** to find out who is using Pegasus for **snooping** on Indians?

iv. How does the government respond to the presence of the Pegasus spyware which was found on the **mobile devices** of certain individuals in India, after the devices had gone through a **technical/forensic analysis**?

Statement of the United Nations High Commissioner

72. On 19.07.2021, the United Nations High Commissioner on Human Rights Michelle Bachelet issued a statement on the Pegasus issue. In the statement she acknowledged that the use of surveillance software had been linked to **arrest, intimidation and even killings of journalists and human rights defenders**. Her statement further said that "*Pegasus spyware, as well as that created by Candiru and others, enable extremely deep intrusions into people's devices, resulting in insights into*

all aspects of their lives, their use can only ever be justified in the context of investigations into serious crimes and grave security threats. A true copy of the statement issued by the UN High Commissioner on Human Rights, dated 19.07.2021 is marked and annexed hereto as **ANNEXURE P-32** ***(Pg. 1223 to 1225).***

73. In a matter of great public significance and of its impact on constitutional rights, the central government has not taken any efforts towards a civic engagement on the issue.

74. That, the Petitioners have understood that in the course of hearing of this petition, the court may require any security to be furnished towards costs or any other charges and the Petitioners shall comply with such requirement.

75. The Petitioners are filing the present Writ Petition before this Hon'ble Court *bona fide* for the welfare and benefit of society as a whole and doesn't have any personal interest in the subject-matter herein. Further, the Petitioners are not involved in any pending civil, criminal or revenue litigation, which has or could have a legal nexus with this petition.

76. That Petitioner No. 2 along with the Center for Public Interest Litigation (CPIL) filed a Public Interest Litigation before the Delhi High Court [W.P. (C) No. 8998 of 2020] challenging surveillance projects CMS, NATGRID and NETRA and this the said PIL is pending adjudication before the Delhi High Court. Notice was issued in the matter to the

Respondents on 02.12.2020. A true copy of the Order passed by the Delhi High Court on 02.12.2020 is marked and annexed as **ANNEXURE P-33** ***(Pg. 1226 to 1227)*****.**

77. That in absence of adequate clarification or transparency on this issue, the Respondents seem to have targeted selected individuals using the pegasus software. Some of these individuals are active in the political sphere and surveillance of their data and their communications raises a question on the legitimacy of the electoral process in India which is the foundation of our democracy.

78. That, the acts of the respondents concerned also violate the principles which were laid down in the Puttaswamy judgment.

79. Upon being extremely dissatisfied and aggrieved by the evasive response and the inaction of the respondents, and the illegal and arbitrary spying of certain individuals, the Petitioner beg to move this Petition under Article 32 of the Constitution of India on following amongst other:

GROUNDS

I. VIOLATION OF THE RIGHT TO FREEDOM OF SPEECH AND EXPRESSION

A. BECAUSE as pointed out in the case of *K.S. Puttaswamy v. Union of India,* (2017) 10 SCC 1 at Para 412, "*Freedom of speech and expression is always dependent on the capacity to think, read and write in private*

and is often exercised in a state of privacy, to the exclusion of those not intended to be spoken to or communicated with." The Pegasus spyware which is presumably being used by the government against its citizens, adopts an invasive technique for snooping on citizens under the garb of national security and public order.

B. BECAUSE in the case of *Tata Press Ltd. Vs. Mahanagar Telephone Nigam Limited and Ors* (1995) 5 SCC 139, this Hon'ble Court observed that: "*Article 19(1)(a) not only guarantees freedom of speech and expression, it also protects the rights of an individual to listen, read and receive the said speech*" (Para 24).

C. BECAUSE as mentioned in the statement issued by the UN High Commissioner for Human Rights Michelle Bachelet, the "*use of surveillance software has been linked to arrest, intimidation and even killings of journalists and human rights defenders. Reports of surveillance also have the invidious effect of making people censor themselves through fear*." Evidently, the use of surveillance has a chilling effect on free speech, leading people to be cautious of their speech, especially speech that is critical of the establishment.

II. VIOLATION OF RIGHT TO FREEDOM OF TRADE AND PROFESSION

D. BECAUSE one of the pre-requisites for a journalist to do his/her job well is to have the much prized anonymity. Journalists in India work under threatening conditions and it is essential for them to know on a daily basis that their communication is not being snooped upon.

E. BECAUSE in the backdrop of the government filing FIRs and sedition cases against journalists and activists, it becomes almost an impossible task for a journalist to do his/her job while knowing that their communications were being checked and monitored by the government. This is an unwarranted and illegal impediment and a violation of the fundamental right to freedom of trade and profession.

F. BECAUSE by virtue of being a civil liberties organization, snooping and surveillance measures through the use of spywares like Pegasus, violates the right to freedom of trade and profession guaranteed to Petitioner No. 2 under Article 19(1)(g) of the constitution of India by creating an unwarranted sense of fear and a chilling effect, dissuading them from being able to do their job freely and fairly.

III. VIOLATION OF ARTICLE 14

G. BECAUSE in on the point of arbitrariness, this Hon'ble Court in the case of *Maeneka Gandhi vs. Union of India and Ors*. AIR 1978 SC 597, has observed: "*The principle of reasonableness, which legally as well as philosophically, is an essential element of equality or non-arbitrariness pervades Article 14 like a brooding omnipresence and the procedure contemplated by Article 21 must answer the best of reasonableness in order to be in conformity with Article 14. It must be "right and just and fair" and not arbitrary, fanciful or oppressive or arbitrary; otherwise, it would be no procedure at all and the requirement of Article 21 would not be satisfied*" (Para 7). An unwarranted and illegal intrusion into citizen's private and personal communications, constitutes an unreasonable and arbitrary act on part of the government.

IV. VIOLATION OF INTERNATIONAL LAW OBLIGATIONS

H. BECAUSE The right to privacy is also recognized as a basic human right under Article 12 of the Universal Declaration of Human Rights Act, 194, which states as follows: "*12. No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, not to attack upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.*"

I. BECAUSE Article 17 of the International Covenant on Civil and Political Rights Act, 1966 to which India is a party, also protects the right to privacy in the following words: "*17. (1) No one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence nor to unlawful attacks on his or her honour and reputation. (2) Everyone has the right to the protection of the law against such interference or attacks*".

J. BECAUSE as the Office of the High Commissioner for Human Rights and the Human Rights Council have emphasized, any interference with privacy must meet standards of legality, necessity and proportionality (A/HRC/27/37, para. 23 and Human Rights Council resolution 34/7, para. 2).

K. BECAUSE the right to privacy is intricately linked with the right to freedom of speech and expression. In a 2015 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (A/HRC/29/32, the Special Rapporteur observed: "*The right to hold opinions without interference also includes the right to form opinions. Surveillance systems, both targeted and mass, may*

undermine the right to form an opinion, as the fear of unwilling disclosure of online activity, such as search and browsing, likely deters individuals from accessing information, particularly where such surveillance leads to repressive outcomes. For all these reasons, restrictions on encryption and anonymity must be assessed to determine whether they would amount to an impermissible interference with the right to hold opinions." The Report further states: "*Privacy interferences that limit the exercise of the freedoms of opinion and expression, such as those described in this report, must not in any event interfere with the right to hold opinions, and those that limit the freedom of expression must be provided by law and necessary and proportionate to achieve one of a handful of legitimate objectives*."

L. BECAUSE as acknowledged by the UN High Commissioner for Human Rights Michelle Bachelet in her statement issued on 19.07.2021, the revelations regarding the apparent widespread use of the Pegasus software to spy on journalists, human rights defenders, politicians and others in a variety of countries are extremely alarming, and seem to confirm some of the worst fears about the potential misuse of surveillance technology to illegally undermine people's human rights. Surveillance measures can only be justified in narrowly defined circumstances, with a legitimate goal, and they must be both necessary and proportionate to that goal.

M. BECAUSE the aforementioned statement further states: "*In addition to immediately stopping their own role in violations of human rights, States have a duty to protect individuals from abuses of the right to privacy by companies*." … "*Governments should immediately cease their own use*

of surveillance technologies in ways that violate human rights, and should take concrete actions to protect against such invasions of privacy by regulating the distribution, use and export of surveillance technology created by others."

N. BECAUSE the United Nations General Assembly, in its resolution 73/179, has emphasized on the principles of legality, necessity and proportionality, and legitimacy. The resolution notes that surveillance of digital communications needs to be consistent with international human rights obligations and must be conducted on the basis of a legal framework, which needs to be publicly accessible, clear, precise, comprehensive and non-discriminatory. (Surveillance and Human Rights Report, 2019) The resolution further mentions : "*States that are parties to the International Covenant on Civil and Political Rights must take the necessary steps to adopt laws or other measures as may be necessary to give effect to the rights recognized in the Covenant*".

O. BECAUSE the Indian government, despite our country being a signatory to it, has negated its responsibility under the International Covenant on Civil and Political Rights (ICCPR). The ICCPR under Article 17, establishes a right to privacy. Article 17(1) states, "*No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.*"

V. DISREGARD FOR THE RULE OF LAW AND THE DEMOCRATIC PROCESSES

P. BECAUSE despite there being stiff opposition, the government has not given a clear response on an issue that has serious consequences on the sustainability and legitimacy of our democratic structure.

Q. BECAUSE the government has maintained complete silence on this issue, while getting cornered in the Parliament, raising further suspicion and insecurity among citizens.

R. BECAUSE the government broke protocol in an unprecedented move where the members of the Parliamentary Committee on IT, did not participate in the Committee meeting which was to be held on 28.07.2021, thereby ensuring with a malicious intent that in the absence of constitution of a quorum, the meeting could not be held.

S. BECAUSE the Respondents have effectively created a situation not very different from an undemocratic and unconstitutional emergency, by curtailing the rights and liberties of a large number of people, on the pretext of public safety and national security.

VI. THE RIGHT TO PRIVACY

T. BECAUSE the right to privacy is a fundamental human right which is fundamental to maintenance of democratic societies.

U. BECAUSE the acts and omissions on part of the Respondents fail to meet the requirements laid down by this Hon'ble Court in the case of *K.S. Puttaswamy vs. Union of India (Privacy-9J)*, (2017) 10 SCC 1. At Para 310 of the said judgment it was observed: "*state must nevertheless put into place a robust regime that ensures the fulfilment of a three-fold 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 re-appreciate 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 three-fold requirement for a valid law arises out of the mutual inter-dependence 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.

V. BECAUSE the Pegasus spyware is a military grade surveillance tool that uses an invasive and inhumane way to spy on its victims. The *Puttaswamy* Judgment at Para 402 aptly states: "*What seems to be essential to privacy is the power to seclude oneself and keep others from intruding it in any way. These intrusions may be physical or visual, and may take any of several forms including peeping over one's shoulder to eavesdropping directly or through instruments, devices or technological aids.*"

W. BECAUSE in the case of *K. S. Puttaswamy vs. Union of India* (2017) 10 SCC 1, this Hon'ble Court observed that "*Privacy" is defined as "the condition or state of being free from public attention to intrusion into or interference with one's acts or decisions*"(Para 402). The Judgment also states: "*The existence of zones of privacy is felt instinctively by all civilized people, without exception. The best evidence for this proposition lies in the panoply of activities through which we all express claims to privacy in our daily lives. We lock our doors, clothe our bodies and set passwords to our computers and phones to signal that we intend for our places, persons and virtual lives to be private.*"(Para 400).

X. BEACUSE on the point limitation of state's authority by constitutional parameters, this Hon'ble Court in the *Puttaswamy* Judgment has observed: "*All liberal democracies believe that the State should not have unqualified authority to intrude into certain aspects of human life and that the authority should be limited by parameters constitutionally fixed.*

Fundamental rights are the only constitutional firewall to prevent State's interference with those core freedoms constituting liberty of a human being. The right to privacy is certainly one of the core freedoms which is to be defended. It is part of liberty within the meaning of that expression in Article 21" (Para 375).

Y. BECAUSE the right to privacy is essential to human dignity and it further reinforces other constitutional rights such as the right to free speech and the right to freedom of association etc.

Z. BECAUSE the right to privacy is an integral part of right to life. This is a cherished constitutional value and it is important that human beings be allowed domains of freedom that are free of public scrutiny unless they act in an unlawful manner.

AA. That this Hon'ble Court had, in *Secretary, Ministry of Information & Broadcasting, Govt. of India and Ors.* v. *Cricket Association of Bengal and Anr.*, [1995] 2 SCC 161, has stated that:

> *"[t]he freedom of speech and expression includes right to acquire information and to disseminate it. Freedom of speech and expression is necessary, for self-expression which is an important means of free conscience and self-fulfilment. It enables people to contribute to debates on social and moral issues, It is the best way to find a truest model of anything, since it is only through it that the widest possible range of ideas can circulate. It is the only vehicle of political discourse so essential to democracy, Equally important is the role it plays in facilitating artistic and scholarly*

endeavours of all sorts. ***The right to communicate, therefore, includes right to communicate through any media that is available*** *whether print or electronic or audio- visual such as advertisement, movie, article, speech etc."* (Para 43)

VII. PROCEDURAL IMPROPRIETY

BB. BECAUSE, not following the procedure prescribed under a statute would render a State action as arbitrary. In *Haresh Dayaram Thakur* v. *State of Maharashtra & Others*, (2000) 6 SCC 179, it was held that "*The position is well settled that if the statute prescribes a procedure for doing a thing, a thing has to be done according to that procedure."* (Para 20). There is no procedure laid down under any law in India that legitimizes or allows the use of an invasive surveillance spyware like Pegasus.

CC. BECAUSE in the case of *Commissioner of Income Tax, Mumbai v. Anjum M. H. Ghaswala & Others*, (2002) 1 SCC 633, it was held by a Constitutional Bench that "[i]t is a normal rule of construction that when a statute vests certain power in an authority to be exercised in a particular manner then the said authority has to exercise it only in the manner provided in the statute itself." (Para 27)

DD. BECAUSE in *State of Uttar Pradesh v. Singhara Singh & Others*, AIR 1964 SC 358, it was held that: "*The rule adopted in Taylor v. Taylor [1875] 1 Ch. D. 426 is well recognized and is founded on sound principle. Its result is that if a statue has conferred a power to do an act and has laid down the method in which power has to be exercised, it*

necessarily prohibits the doing of the act in any other manner than that which has been prescribed. The principle behind the rule is that if this were not so, the statutory provision might as well not have been enacted." (Para 8) As pointed out in this Petition, there have been multiple incidents of illegal electronic surveillance. This substantiates the fact that the government inadvertently or with involvement of some of its functionaries, is known to have not been able to safeguard citizens against illegal and unconstitutional intrusion into their right to privacy.

VIII. LACK OF JUDICIAL OVERSIGHT

EE. BECAUSE the current process of oversight entails the executive keeping a check on the executive. As evidenced by multiple instances in the past, this enhances the scope for misuse and reduces the scope for keeping a check on the excesses committed by the Executive.

FF. BECAUSE the AP Shah Committee Report highlighted the problem of lack of a judicial oversight in the following words:

> "***The regime does not require judicial oversight or authorization****, it is unclear which agencies are legally authorized to undertake interception/access, systematic access or proactive disclosure of communications and classes of data is not prohibited, agencies are not required to be transparent to the public regarding the effectiveness and cost of each intercept, interception/access is permitted for even minor offenses, there is no requirement for standardization of orders, there are no additional safeguards for when interceptions/access invade individual's privacy beyond the targeted subject, and the individual is never notified that an*

interception/access took place, even after the close of the investigation." (emphasis supplied)

GG. BECAUSE as a consequence of lack of judicial oversight, individuals who have incorrectly been subjected to surveillance or have been subjected to illegal or unauthorized surveillance, are not given any information in respect of them being subjected to unauthorized or illegal surveillance.

HH. BECAUSE the United Nations in the U.N. General Assembly Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/RES/73/179 (17 December 2018) has emphasized on the importance of judicial oversight in the following words: "*6. Calls upon all States: (d) To establish or maintain existing* ***independent, effective, adequately resourced and impartial judicial, administrative and/or parliamentary domestic oversight mechanisms capable of ensuring transparency****, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data;*"

II. BECAUSE the Human Rights Committee of the United Nations, in its Concluding observations on the fifth periodic report of Belarus, Human Rights Committee, U.N. Doc. CCPR/C/BLR/CO/5 (22 November 2018) has stressed upon the importance of a judicial oversight in the following words: "*44. The State party should ensure that: ... (b) surveillance and interception is conducted subject to judicial authorization as well as effective and independent oversight mechanisms; ...*"

JJ. BEACUSE The International Principles on the Application of Human Rights to Communications Surveillance stress that "*Determinations related to Communications Surveillance must be made by a competent judicial authority that is impartial and independent. The authority must be*:

1. separate and independent from the authorities conducting Communications Surveillance;

2. conversant in issues related to and competent to make judicial decisions about the legality of Communications Surveillance, the technologies used and human rights; and

3. have adequate resources in exercising the functions assigned to them.

IX. OVERBROAD POWERS FOR MONITORING UNDER SECTION 69 OF THE INFORMATION TECHNOLOGY ACT, 2000

KK. BECAUSE Section 69 of the Information Technology Act provides the Central Government and State Governments the power to issue directions for interception or monitoring or decryption of any information through any computer resource even for the investigation of any offence. This is in contrast with Section 5(2) of the Telegraph Act where an order for telephone tapping can be issued only on the occurrence of any public emergency, or in the interest of public safety. This condition is absent in the case of Internet monitoring under Section 69 of the IT Act, 2000. The threshold for issuing a monitoring order under the IT Act is so low that this could be issued in relation to investigation of any offence. In the current scenario, when the use of

mobile phones and internet communications are so widespread, such an order will have a greater impact than a telephone tapping order. Section 69 of the Information Technology Act to the extent it provides for issuing of directions for interception or monitoring or decryption of any information for investigation of any offence is illegal and violative of Art.14, 19 and 21 of the Constitution of India.

X. INADEQUACY OF THE CURRENT SURVEILLANCE FRAMEWORK

LL. BECAUSE multiple instances of illegal surveillance, some of which have been captured in this Petition, indicate that the current surveillance framework in India lacks the requisite safeguards for protection against illegal and unwarranted intrusion of citizens' privacy through surveillance.

MM. BECAUSE the erstwhile Minister of Communications and Information Technology Shri Ravi Shankar Prasad has stated before the Lok Sabha that "*on an average 5000 interception orders per month are issued by the Union Home Secretary on the requests supported by justified grounds/ reasons made by Law Enforcement Agencies*." It is pertinent to mention that this admission by the government highlights the inherent fallacy in the authorization mechanism for communication surveillance in India. The Secretary in the Ministry of Home Affairs in the Central Government has the responsibility for authorizing requests for the interception, monitoring, and decryption of communications issued by Central agencies, and the Secretary in charge of the home department is responsible for authorizing requests for the interception,

monitoring and decryption of communications from state level agencies and law enforcement. It is questionable as to how the union home secretary in this case would be able to peruse, apply his/her mind and then make a sound decision in respect of so many Orders, given the fact that he/she also shoulders many other responsibilities. The proportionality test encapsulates within itself the element of necessity which means that interception of communication should only be done when it is the least restrictive way of achieving a legitimate purpose. It is not very clear if that principle is being applied when a total of 5000 Orders are being issued per month.

NN. BECAUSE In absence of sufficient clarity from the government, coupled with the alarming set of facts and accompanying evidence, it is evident that the government has used the Pegasus malware to spy on its citizens. Since such surveillance is beyond the existing framework of lawful and interception monitoring under the Telegraph Act, 1885 and the IT Act, 2000 and the accompanying rules, adequate safeguards must be placed to ensure such incidents don't occur in the future.

OO. BECAUSE under the existing lawful interception and monitoring framework, if a person falls victim to unlawful or unwarranted surveillance by the state, he or she has no recourse or remedy under the law to seek corrective action or demand compensation for the loss or injury suffered.

PP. BECAUSE the Data Protection Bill exempts the government or any of its agencies from the requirements of the legislation. This enhances the scope of surveillance and reduces the safeguards against an abuse of

surveillance and increases the risks of human rights violations like the one that has happened in the Pegasus case.

XI. UNCHECKED GROWTH OF PRIVATE SURVEILLANCE COMPANIES

QQ. BECAUSE as highlighted in this Petition, there has been a staggering growth of private surveillance companies which are operating in India and are manufacturing and selling surveillance technologies in India.

RR. BECAUSE private surveillance companies operate in a regulatory grey area, with little to no transparency or accountability in terms of their operations and the impact of their work on human rights abuses.

SS. BECAUSE there is no clarity on whether or not private surveillance technology companies are required to conduct a due diligence or a human rights assessment before selling surveillance technologies to law enforcement agencies. The legality of operations of such private surveillance companies is entirely questionable in view of the fact that the Information Technology Act expressly criminalizes the infiltration and discreet retrieval of information of the nature discussed above. The possibility of government collusion only makes matters worse as LEAs seemingly have no qualms in skirting the law to procure desired information, leaving citizens none the wiser. Additionally, the discreet nature of these endeavours means there is no public accountability or oversight involved whatsoever. After the Pegasus revelation, every citizen is left to grapple with the rather unsettling question of what other discreet surveillance mechanisms are currently in deployment that we

haven't had the fortune of coming to know of through chance encounters at security conferences.

TT. BECAUSE the proliferation of private surveillance tech companies in India and around the world, has seen an unchecked growth in the past few years and the said entities operate in a regulatory grey area.

XII. NEED FOR FRAMING OF GUIDELINES

UU. BECAUSE the current legal framework is based on the PUCL guidelines framed by this Hon'ble Court. Both Rule 419A of the Telegraph Rules, 1951 as well as the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 are modelled on the PUCL guidelines and have similar procedures for issuance of tapping/monitoring orders and for reviewing these orders which are collectively and individually, grossly inadequate.

VV. BECAUSE the judgment in *People's Union for Civil Liberties (PUCL) v. Union of India*, was passed at a time when landline telephones were the predominant means of communication. Mobile services were introduced in 1995 and were not very common at that time. The methods of communication have changed drastically since then, necessitating an overhauling of the lawful interception and monitoring framework in India. A mobile phone is a virtual extension of the citizen as it is carried by her throughout the day. Access to such a device has great implications for the rights of the person as the phone contains intimate details of the person including her conversations, photographs, health details, financial details and official communications that could have trade secrets.

WW. BECAUSE with the advancement of communication technology and the accompanying growth in the potential for misuse or arbitrary exercise of power, there needs to be adequate checks and balances upon the executive, to ensure citizens are protected against unwarranted intrusions into their right to privacy.

XX. BECAUSE the monitoring of modern devices should only be permitted after ensuring that the process of interception and monitoring passes the test of necessity and proportionality, and is vetted by the application of a judicial mind. This is in line with the adoption of best practices from around the world, wherein an order from a judge is a prerequisite for initiating the process of interception or surveillance.

YY. BECAUSE even though the PUCL Guidelines were essential and indispensable at the time of its coming into existence, this Hon'ble court while drafting the guidelines, had termed it to be a "temporary solution." Furthermore, the Guidelines did not contemplate a much needed judicial oversight mechanism, in order to safeguard against arbitrary exercise of power by the executive.

XIII. NEED FOR A COURT MONITORED INVESTIGATION

ZZ. BECAUSE in the case of *Ram Jethmalani and Othrs vs. Union of India and Othrs.* (2011) 8 SCC 1, this Hon'ble court observed: "We note that in many instances, in the past, when issues referred to the Court have been very complex in nature, and yet required the intervention of the Court, Special Investigation Teams have been ordered and constituted in order to enable the Court, and the Union of India and/or other organs of the State, to fulfil their constitutional obligations. "(Para 56)

AAA. BECAUSE in the case of *Romila Thapar and Othrs vs. Union of India and Othrs* (2018) 10 SCC 753, Justice Chandrachud in his dissenting opinion has observed: "*Over the course of the last decade, the jurisdiction of this Court has evolved under Article 32 to Order the constitution of a SIT. In NHRC v. State of Gujarat, a SIT was constituted in a matter involving a serious element of communal disharmony. Further directions were issued by this Court for regular status reports to be filed by the SIT (NHRC v. State of Gujarat). In Ram Jethmalani v. Union of India, this Court observed that in several instances in the past, when the issue were of a complex nature, yet requiring the intervention of the Court, SITs were ordered to be constituted to enable the Court, the Union Government and other organs of the state to fulfil their constitutional obligations. In Common Cause v. Union of India, the test for the constitution of SIT was a prima facie abuse of power and authority by the Director of the Central Bureau of Investigation to scuttle an investigation and enquiries into coal block allocations. In Sunita Devi v. Union of India, an independent and impartial SIT was constituted where it was found that the investigation into the murder of a family was lackadaisical and the real culprits had not been put to trial. These instances indicate the diversity of settings in which this Court has ordered the constitution of SITs*. (Para 67).

BBB. BECAUSE this Hon'ble Court in the aforementioned judgment has further observed: "*Decisional flexibility in the exercise of this jurisdiction meets exigencies which arise in unforeseen situations, warranting the intervention of this Court under Article 142. While the Court does not determine the course of the investigation, it acts as a*

watchdog to ensure that a fair and impartial investigation takes place. A fair and independent investigation is crucial to the rule of law and, in the ultimate analysis to liberty itself." (Para 67)

CCC. BECAUSE an investigation into an issue cannot be unbiased and fair if the Central Government and its agencies are under the shadow of suspicion, as they are in this case. It therefore becomes imperative that considering the peculiar set of circumstances, an independent investigation which is either appointed and/or monitored by this Hon'ble Court, must be done.

38. That the Petitioners state that in the facts and circumstances stated hereinabove, he has made out a strong prima facie case which warrants judicial review.

39. That the balance of convenience and/or inconvenience rests in favour of the Petitioners for grant of reliefs as prayed for hereinafter and such reliefs, if granted, would provide adequate remedy to the petitioner and the public at large.

40. That the Public at Large shall suffer irreparable loss, injury and prejudice if orders as prayed for hereinafter are not granted.

41. That the Petitioners have not approached any other Court or any other forum seeking redressal of the same cause of action.

42. This application is bonafide and made in the interest of justice

43. That the Petitioners have not filed any similar petition seeking similar reliefs before any High Court or before this Hon'ble Court.

PRAYER

In light of the facts and circumstances of this case, the Petitioners pray before this Hon'ble Court as under:

a) For a writ of mandamus or any other appropriate Writ or order directing the Union of India, all State Governments and all public bodies and authorities to not have any dealings with NSO and to discontinue all dealings with NSO, effectively banning NSO from any activities in or in connection with India.

b) For an order prohibiting the Government of India, all State Governments and all public bodies and authorities from outsourcing/sub-contracting any surveillance activity to the private sector in any manner, and directing discontinuation of all such dealings.

c) For a writ of mandamus or any other appropriate Writ or order directing the Union of India to completely stop all surveillance activity conducted by private parties in India.

d) For a writ of mandamus or any other appropriate Writ or order directing the Union of India to establish a judicial oversight mechanism for issuance of any surveillance order

e) Issue guidelines covering the following aspects:

i. Establishment of a judicial oversight mechanism under the existing lawful interception and monitoring framework within the Telegraph Act, 1885 and the Information Technology Act, 2000 by designating Courts for approval of interception/monitoring orders.

ii. Ensuring that surveillance orders are issued complying with the principles of necessity and proportionality and after considering other less intrusive alternatives.

iii. Conduct a periodic human rights impact assessment in respect of all surveillance mechanisms introduced by the government.

iv. Ensuring transparency of surveillance orders issued with proper oversight and access to records by a Parliamentary Committee.

v. Ensuring notification to the subject of surveillance after completion of the period of surveillance.

f) Order an investigation/probe which is monitored by this Hon'ble Court on the use of the Pegasus spyware for surveillance of Indian citizens, which is conducted by officers chosen by this Hon'ble Court who are independent of the Union of India.

g) Issue a writ in the nature of mandamus directing the Respondents to make public, the following details in respect of the business arrangement of Government of India with the Israeli company NSO:

i. Whether there existed any arrangement with NSO for the purchase or use of the Pegasus spyware by the Government of India or any of its agencies or by any of the state governments or any of its entities.

ii. The cost of sale of the Pegasus spyware and/or the cost of using the Pegasus spyware to spy per mobile device.

iii. Sets of information about Indian citizens which were provided to the NSO group in furtherance of carrying out surveillance using the Pegasus spyware.

iv. The framework which was agreed upon between the Government of India and the NSO Group for keeping the data of Indian citizens who were being spied on.

v. Involvement of any third party in the arrangement between Government of India and the NSO group.

vi. The number of people and mobile devices which were sought to be targeted under the arrangement.

vii. Details in respect of the dispute resolution mechanism and the jurisdiction that was agreed upon by the parties.

viii. Details in respect of any investigation conducted by Respondent No. 2 and/or 3 regarding the WhatsApp vulnerability misused by NSO for gaining entry to targeted devices by the Pegasus software

h) For an order, writ or direction declaring Rule 419A of the Indian Telegraph Rules, 1951 as unconstitutional, void and violative of Articles 14, 19 and 21 of the Constitution of India.

i) For an order, writ or direction declaring Section 69 of the Information Technology Act, 2000 as unconstitutional, void and violative of Articles 14, 19 and 21 of the Constitution of India. ,

j) For an order, writ or direction declaring the provisions of Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 as unconstitutional, void and violative of Articles 14, 19 and 21 of the Constitution of India.

k) Any other or further order or orders, direction or directions as this Hon'ble Court may deem fit and proper;

And for this act of kindness, the petitioner as in duty bound shall ever pray.

Drawn on: 09.08.2021

Drawn by:

Mishi Choudhary

Prasanth Sugathan

Kushagra Sinha

Siddharth Seem

Filed on: 09.08.2021

Filed by:

Advocate for the Petitioners