IN THE HIGH COURT OF DELHI AT NEW DELHI

EXTRA ORDINARY CIVIL ORIGINAL JURISDICTION

WRIT PETITION (C) NO. _____ OF 2020 (P.I.L)

IN THE MATTER OF PUBLIC INTEREST LITIGATION:

CENTRE FOR PUBLIC INTEREST LITIGATION &

ANOTHER PETITIONERS

VERSUS

UNION OF INDIA & OTHERS RESPONDENTS

WRIT PETITION UNDER ARTICLE 226 OF THE CONSTITUTION OF INDIA FOR A WRIT OF MANDAMUS OR ANY OTHER APPROPRIATE WRIT, ORDER, OR DIRECTION TO THE RESPONDENTS TO PERMANENTLY STOP THE EXECUTION AND THE OPERATION OF THE SURVEILLANCE PROJECTS NAMELY "CMS", "NETRA", AND "NATGRID" WHICH ENABLES FOR MASS/BULK INTERCEPTION, STORAGE, ANALYSIS, AND RETENTION OF TELEPHONE AND INTERNET COMMUNICATIONS DATA; AND FURTHERMORE, TO DIRECT FOR CONSTITUTING A PERMANENT INDEPENDENT OVERRSIGHT AUTHORITY - JUDICIAL AND/OR PARLIAMENTARY BODY TO AUTHORIZE AND REVIEW INTERCEPTION AND MONITORING ORDERS/ WARRANTS ISSUED UNDER THE ENABLING PROVISIONS OF TELEGRAPH ACT, 1885 AND THE INFORMATION TECHNOLOGY ACT, 2000, CONFORMING TO THE PRINCIPLES AND REASONABLE RESTRICTINGS AS LAID DOWN BY THE HON'BLE SUPREME COURT IN CASE TITLED K.S. PUTTASWAMY & ORS. V UNION OF INDIA (2017) 10 SCC 1;

SYNOPSIS

The Petitioners are filing the instant writ petition in public interest under Article 226 of the Constitution of India, for the enforcement of fundamental right to privacy of Indian Citizens emanating from Article 21 and wide ranging freedoms guaranteed under Part III of the Constitution of India, endangered by the execution and operation of Surveillance Projects by the respondents, namely *Centralized Monitoring System* ("**CMS**"), *Network Traffic Analysis* ("**NETRA**"), and *National Intelligence Grid* ("**NATGRID**"). The Surveillance Projects allows the authorized central and state law enforcement agencies to intercept and monitor all and any Telecom and Internet Communications in bulk, leading to a mass illegal dragnet surveillance system by the state, thereby infringing the fundamental right to privacy of individuals, and furthermore, exceeds the Constitutional restrictions, principles, and adequate safeguards laid down by the Hon'ble Supreme Court in the landmark cases of *K.S. Puttaswamy & Ors. vs. Union of India* ("*Privacy Judgement*"), reported in *(2017) 10 SCC 1* and in *People's Union of Civil Liberties (PUCL) v. Union of India &Anr.* reported in *(1997) 1 SCC 301*.

Additionally, under the existing legal framework, there is an **insufficient oversight mechanism** to authorize and review the interception and monitoring orders issued by the state agencies under section 5(2) of the Indian Telegraph Act, 1885

read with Rule 419(A) of the Indian Telegraph (Amendment) Rules, 2007. As per the RTI reply dated 12.05.2014 obtained from the Central Public Information Officer (**CPIO**), Ministry of Home affairs, Government of India, it is submitted that on an average, around 7500 – 9000 telephone-interception orders per month were being issued by the Central Government alone during 2013-2014 period. Such huge number of interception orders when issued by the Central and State Authorities in a massive and disproportionate scale, can only be said to be issued in a mechanical manner without application of mind, thereby exceeding the adequate procedural safeguards and oversight mechanism under Indian Telegraph Act, 1885 and Indian Telegraph (Amendment) Rules 2007, which were issued in compliance to the guidelines laid down by the Hon'ble Supreme Court in the*PUCL vs. Union of India*(supra), which laid the groundwork for the right to privacy in the context of telephonic surveillance (i.e. wiretaps) and constitutional freedoms.

Furthermore, the existing review mechanism introduced under Rule 419(A) of Indian Telegraph (Amendment) Rules, 2007 on the basis of the law laid down in *PUCL vs. Union of India* (supra), in the form of the review committee chaired by the Cabinet Secretary at the Central Government level and Chief Secretary at the State Government level, consists entirely of the officials from the executive branch, without any

parliamentary or judicial oversight, resulting in the lack of transparency and accountability. This lack of adequate independent oversight mechanism to authorize and review the lawful authorizations of interception and monitoring of individuals infringes the fundamental right to privacy and procedural safeguards as laid down by the Hon'ble Supreme Court in the Puttaswamy*Privacy* Judgement reported as *(2017) 10 SCC 1.*

1. Centralized Monitoring System (**CMS**) Project:

On 26.11.2009, the Press Information Bureau, Government of India has provided details of the **CMS** project, as a centralized system to monitor communications on mobile phones, landlines and Internet traffic in the country, in order to "strengthen the security environment in the country". The Minister-in-charge of State in the Ministry of Communications and Information Technology, Government of India in his answers to unstarred question No. 3207 asked in the Lok Sabha on 12.12.2012, and unstarred question No. No.1598 asked in the Rajya Sabha on 23.08.2013, has submitted that the **CMS** project has been approved by the Cabinet Committee on Security (CCS) in its meeting held on 16.06.2011, and further confirmed the completion of its development work and pilot trial in Delhi by integrating interception services under CMS project with Telecom Service Providers (TSPs) by date 30.09.2011; and that the features of **CMS** project included -

Central and Regional databases that would help Law Enforcement Agencies ("LEAs") in the interception and monitoring; Direct Electronic Provisioning of targeted numbers by state agencies without any manual intervention from the Telecom Service Providers ("TSPs"); creation of filters and alerts on targeted numbers; Call Data Records ("CDR") analysis; data mining on CDRs to collect metadata - call details, location details, etc. of the targeted numbers; and conducting Research & Development in related fields for continuous upgradation of the speculative profiles of the CMS.

In a recent answer provided by the Minister-in-charge to Unstarred Question No. 1440 in Rajya Sabha dated 04.07.2019, it is stated that that the Centralised Monitoring Centre (CMC) at Delhi and all the 21 Regional Monitoring Centres (RMCs) have been operationalised under CMS project, thereby effectively covering all the 22 Licensed Service Areas across the country.The Ministry of Communications, Department of Telecommunications, Government of India in its reply letter dated 08.01.2020 to an RTI query, has affirmed that the **CMS** project is currently operational, and its functioning along with the applicable safeguards for preventing misuse of data collected through CMS project is as under Rule 419-A of the Indian Telegraph Rules 1951.

The reported objectives, functional aspects, and phase of execution confirmed through parliamentary answers and RTI reply dated 08.01.2020 regarding **CMS** project, leads to an unambiguous conclusion that the Government has completed the operationalization of the project effectively covering the entire country, and consequently the Central and State Law Enforcement Agencies (LEAs) have a direct and easy access to intercept, monitor, store, and analyse all and any Telecom and Internet communications in bulk, thereby infringing the fundamental right to privacy of many individuals emanating from Articles 14, 19(1), and 21 of the Constitution, without conforming to the constitutional restrictions, safeguards and proportionality standards as laid down in the judgement by the Hon'ble Supreme Court in Puttaswamy (Privacy-9j) case. The functional features of the CMS project allows for the state and authorized agencies to bypassthe existing procedural safeguards to be followed while issuing Lawful Interception and Monitoring orders (LIMs) under the relevant statutory provisions and Rules of the *Indian Telegraph Act, 1885* and *Information Technology Act, 2000.*

2. Network Traffic Analysis **(NETRA)** Project:

The Network Traffic Analysis ("**NETRA**) was developed by Centre for Artificial Intelligence ("**CAIR**"), a lab under Defence Research and Development Organization ("**DRDO**") to monitor Internet traffic for the use of keywords such as 'attack', 'bomb',

'blast' or 'kill' in tweets, status updates on social media platforms, emails or blogs. As per the reports, NETRA storage servers known as 'nodes' would be installed at an Internet Service Provider's level at more than 1000 locations across India, each with a storage capacity of 300 GB, thus totalling 300TB for storage, retention, and analysis.

NETRA is essentially a massive dragnet surveillance system designed specifically to monitor the nation's Internet networks including voice over internet traffic passing through software programs such as Skype or Google Talk, besides write-ups in tweets, status updates, emails, instant messaging transcripts, Internet calls, blogs and forums.

3. National Intelligence Grid **(NATGRID)** Project:

The National Intelligence Grid ("**NATGRID**") is portrayed as an ambitious counter-terrorism initiative to be undertaken on public-private partnership that will utilize technologies like Big Data and advanced analytics to study and analyze huge amounts of data and metadata related to individuals from various standalone databases belonging to various agencies and ministries of the Indian Government, which includes tax and bank account details, credit card transactions, visa and immigration records and itineraries of rail and air travel.

Government of India has set up National Intelligence Grid (NATGRID), as an attached office of the Ministry of Home Affairs with effect from 01.12.2009. NATGRID, a department under the Respondent No. 3, Ministry of Home Affairs in a reply under the Right to Information Act, 2005 by CPIO (NATGRID) on date 09.06.2011, stated that Security agencies can seek the details from the NATGRID database, and that the data from Airline companies, Telecom companies, etc. would be uploaded to NATGRID database. However, shortly after this reply, NATGRID was placed out of purview of RTI Act, 2005 vide Gazette Notification No. 442(E) dated 9.6.2011. It is submitted that the Ministry of Home Affairs (Respondent No. 3) has responded to an unstarred question No. 437 in Lok Sabha on 19.11.2019 regarding NATGRID, confirming that the NATGRID project will be made operational by date 31.12.2020. The Minister in his reply has further stated that during the current financial year of 2019, Rs. 84.80 Crore has been allocated for NATGRID Project, and against 119 sanctioned Government Posts, a total of 53 officers are presently in position; whereas against 123 contractual posts, 21 consultants have been deployed; and that the Central Agencies will have access to the data on NATGRID platform in the first phase.

NATGRID project results in a real-time profiling of individuals through collection, aggregation, and analysis of metadata of

individuals, which could reveal information such as civil, political, religious affiliation; social status; support to a charitable organization; subject's involvement in an intimate relationship, etc..

The recent reports of targeted surveillance attack via the **'WhatsApp'** application on mobile phones of 121 lawyers and social activists using **Pegasus** malware/spyware and the Central Government's denial to provide a clear response regarding any contractual engagement with the NSO Group, before the Hon'ble Parliament of India is a clear display of unlawful and vested use of surveillance machinery exploited under complete absence of judicial oversight and procedural safeguards. The Hon'ble Supreme Court in the *K.S. Puttaswamy (Privacy-9J.) v. Union of India, (2017) 10 SCC 1* has held that in the ultimate analysis, the balancing act that is to be carried out between individual, societal and State interests must be left to the training and expertise of the judicial mind, when the State action infringes the fundamental right to privacy.

Thus, based on the facts aforementioned with corroborating documents, the Surveillance Projects namely "CMS", "NETRA", and "NATGRID", which allows for unbridled collection, processing, and storage of huge amounts of personal data pertaining to individuals, violates the basic fundamental right

to privacy, and are ultra vires to Articles 14, 19(1)(a) and 21 of the Constitution of India. These Surveillance Projects coupled with the inadequate oversight mechanism allows the State law enforcement agencies to subject all and any individual under mass surveillance for any amount of time, thereby subordinating the individuals' dignity and liberty to the power of the State, thus violating the basic fundamental right to privacy enshrined in the Articles 19(1)(a) and 21 of the Constitution, as the established law laid by the Hon'ble Supreme Court in the *K.S. Puttaswamy (9J-Privacy)* Judgement.

Hence, this writ petition has been filed by the petitioners in the Hon'ble High Court at Delhi.

LIST OF DATES

Date	Particulars
2007-08	Annual Report of the Department of Telecommunications ("**DoT**") states finalization of requirements of Centralized Monitoring System ('CMS') Project.
26.11.2009	Centralized Monitoring System ("**CMS**") Project publicly announced with a press release by Press Information Bureau.
16.07.2011	CMS Project approved by the Cabinet Committee on Security.
06.06.2011	Response to RTI request by Petitioner No. 2 providing Cabinet Committee's decision on

	Security stating establishment of NATGRID under Union Ministry of Home Affairs.
09.06.2011	Reply to an RTI application sent by the Central Public Information Officer (**CPIO**) stated that Security agencies can seek the details from the NATGRID database. It is further stated that data from Airline companies, Telecom companies, etc. would be uploaded to NATGRID database.
09.06.2011	NATGRID was placed out of purview of RTI Act, 2005 vide Gazette Notification No. 306.
February, 2012	Reports of setting up of NETRA to monitor Internet traffic on real-time basis.
October, 2012	Justice A. P. Shah Committee submits 'Report of the Group of Experts on Privacy'.
12.12.2012	Unstarred question 3207 asked in the Lok Sabha pertaining to the intention of the Government of setting up of CMS and its features thereof. Shri Milind Deora answered the question in positive about the Government's intention to set up CMS for interception of telephone and internet services. The salient features of the CMS shall include setting up of central and regional databases to facilitate monitoring and interception by the Central and the State Level Law Enforcement Agencies as well as give access to these agencies of Cell Data Records.
May, 2013	Edward Snowden, a former NSA/CIA subcontractor revealed around 10,000 documents to *the Guardian* journalist Glenn Greenwald and Ewen MacAskill, and documentary filmmaker Laura Poitras which exposed various illegal mass surveillance

	programmes that were run by the Government of the United States partnering along with other national governments.
13.06.2013	Amendments made to Unified Access Service License ("**UASL**") and Unified License ("**UL**") in order to connect the existing monitoring centres to the CMS network. As per the amendments, the service providers need to provide dark optic fiber connectivity at their own cost up to the nearest point of presence of the CMS network.
23.08.2013	Unstarred question No.1598 asked in the Rajya Sabha as to whether the data gathered through the CMS is retained by the agencies or shared with third parties and if so, for how long. Shri Milind Deora answered that the records pertaining to the directions for interception and of intercepted messages shall be destroyed by the relevant competent authority and agencies every 6 months unless, these are required for functional requirement.
08.02.2014	The Ministry of Communications And Information Technology vide official Gazette Notification dated 08.02.2014 has amended Rule 419A of the Indian Telegraph Rules 1951.
01.02.2014	Article titled "How Edward Snowden went from loyal NSA contractor to whistle-blower" stated that the Snowden revelations disclosed that the United States conducted surveillance on citizens of other countries also. Of the countries spied upon, India was among the top targets.
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	Resolution on Right to Privacy in the Digital Age adopted by United Nations General Assembly.
24.08.2017	Hon'ble Supreme Court in **Justice K. S. Puttaswamy (Retd.) and Anr. vs Union Of India And Ors** (W.P. (C) No. 494 of 2012) upholds Right to Privacy as a Fundamental Right.
18.09.2018	Release of the Citizen Lab's Report titled "**Hide And Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries**" revealing the use of Pegasus malware/spyware to conduct surveillance in 45 Countries, including India.
24.06.2019	The Citizen Lab, a Toronto based independent research community has released an article titled "*The Dangerous Effects of Unregulated Commercial Spyware*" highlighting a chilling trend observed elsewhere, whereby the political opponents, Human Rights organizations and Lawyers, journalists and members of civic media are disproportionately targeted with powerful spyware technologies, and thereby calling for a an immediate moratorium on the global sale and transfer of the tools of the private surveillance industry until rigorous human rights safeguards are put in place to regulate such practices and guarantee that governments and non-state actors use the tools in legitimate ways.
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) judgement and has 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.
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.
19.11.019	Unstarred Question No. 437 asked in the Lok Sabha pertaining to the present status of NATGRID and if it is operational already and if not, the time frame within which it shall become operational. Shri G. Kishan Reddy stated that the Physical infrastructure of NATGRID is planned to be completed by 31.03.2020 and it is planned to go live by 31.12.2020 and it is exempted from the RTI Act, 2005.
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.
27.12.2019	Ministry of Home Affairs, Cyber and Information Security Division (CIS Division/ CIS-III Desk), Government of India in its reply dated 27.12.2019 to an RTI question, has confirmed that the NATGRID project has been exempted from the RTI Act, 2005 vide Gazette of India Notification No. GSR 442 € dated 09.06.2011 issued by DoP&T.
08.01.2020	The Ministry of Communications, Department of Telecommunications, Government of India in its reply letter dated 08.01.2020 to an RTI query, has affirmed that the **CMS** project is currently operational, and its functioning along with the applicable safeguards for preventing misuse of data collected through CMS, is as under Rule 419-A of the Indian Telegraph Rules 1951.

IN THE HIGH COURT OF DELHI AT NEW DELHI

EXTRA ORDINARY CIVIL ORIGINAL JURISDICTION

WRIT PETITION (C) NO. _____ OF 2020 (P.I.L)

IN THE MATTER OF PUBLIC INTEREST LITIGATION:

CENTRE FOR PUBLIC INTEREST LITIGATION & ANOTHER PETITIONERS

VERSUS

UNION OF INDIA & OTHERS RESPONDENTS

WRIT PETITION UNDER ARTICLE 226 OF THE CONSTITUTION OF INDIA FOR A WRIT OF MANDAMUS OR ANY OTHER APPROPRIATE WRIT, ORDER, OR DIRECTION TO THE RESPONDENTS TO PERMANENTLY STOP THE EXECUTION AND THE OPERATION OF THE SURVEILLANCE PROJECTS NAMELY "CMS", "NETRA", AND "NATGRID" WHICH ENABLES FOR MASS/BULK INTERCEPTION, STORAGE, ANALYSIS, AND RETENTION OF TELEPHONE AND INTERNET COMMUNICATIONS DATA; AND FURTHERMORE, TO DIRECT FOR CONSTITUTING A PERMANENT INDEPENDENT OVERRSIGHT AUTHORITY - JUDICIAL AND/OR PARLIAMENTARY BODY TO AUTHORIZE AND REVIEW INTERCEPTION AND MONITORING ORDERS/ WARRANTS ISSUED UNDER THE ENABLING PROVISIONS OF TELEGRAPH ACT, 1885 AND THE INFORMATION TECHNOLOGY ACT, 2000, CONFORMING TO THE PRINCIPLES AND REASONABLE RESTRICTINGS AS LAID

DOWN BY THE HON'BLE SUPREME COURT IN CASE TITLED K.S. PUTTASWAMY & ORS. V UNION OF INDIA (2017) 10 SCC 1;

TO,
THE HON'BLE CHIEF JUSTICE AND
THE OTHER COMPANION JUDGES OF
THE HON'BLE HIGH COURT OF DELHI

THE HUMBLE PETITION OF THE PETITIONERS ABOVE-NAMED MOST RESPECTFULLY SHOWETH:

1) That the petitioner organizations filing the instant writ petition in public interest. The petitioners have no personal interest in the litigation and the petition is not guided by self-gain or for gain of any other person / institution / body and that there is no motive other than of public interest in filing this writ petition.

2) That the facts alleged in present writ petition have been sourced from public domain and from information received from the members of the petitioners' organization.

3) That the petition, if allowed, would ensure the protection of Fundamental Right to Privacy emanating from Articles 19(1), 21 and other fundamental rights enshrined under Part III of the Constitution of India, of many citizens of the country by directing the respondents to permanently stop the operation and execution of functional surveillance mechanisms and projects ('Surveillance Projects') namely Centralized Monitoring System ('CMS'), Network Traffic Analysis ('NETRA') and National Intelligence Grid

('NATGRID') which allows for a mass surveillance state by issuing orders for the unauthorised and illegal collection of any data of any individual. Hence, the petitioners herein prefer this Public Interest Litigation.

4) The only affected parties by the orders sought in this writ petition would be the Respondents. To the best of the knowledge of the petitioner, no other persons /bodies /institutions are likely to be affected by the orders sought in this writ petition.

(Antecedents of the Petitioners)

5) A. That the Petitioner No. 1 is a registered society formed for the purpose of taking up causes of grave public interest and conducting public interest litigation in an organized manner. Its founder President was the late Shri V.M. Tarkunde and founder members consisted of several senior advocates including Shri Fali S. Nariman, Shri Shanti Bhushan, Shri Anil Divan, Shri Rajinder Sachar, Shri Colin Gonsalves among others. Ms. Kamini Jaiswal is the General Secretary of the petitioner No.1 and is authorized to institute petitioners on behalf of the petitioner no. 1. The office address of petitioner no.1 is 43, Lawyer's Chambers, Supreme Court of India, New Delhi-110001. The petitioners has means to pay if any cost is imposed by the Hon'ble Court.

B. That the Petitioner No. 2 is a registered society under the Societies Registration Act, 1860 bearing registration

number S-68628 dated 03-03-2010 that works for the promotion and protection of digital rights and digital freedoms. Petitioner No. 2 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. 3 has researched and published multiple reports in support of the freedom of speech and expression including on issues such as Internet shutdowns, online harassment and intermediary liability, and tracks instances of violation of freedom of speech and expression through censorship in the country.

6) That, there are violations of fundamental rights such as the right to equality, right to freedom of speech and expression, right to privacy, right to life and personal liberty to live with dignity guaranteed under Articles 14, 19, and 21 of the Constitution of India while executing Surveillance Projects.

7) That, the present petition under Article 226 of the Constitution of India is being filed by way of Public Interest Litigation and the Petitioners have no personal interest herein. This petition is being filed in the interest of the public at large and with a view to bring the existing surveillance projects under judicial scrutiny for protection

of fundamental rights under the Constitution of India and establishing adequate safeguards.

8) That, thorough research has been conducted in the matter raised through the present Public Interest Litigation and the relevant available matters in this regard are being annexed herewith.

9) That, to the best of the Petitioners' knowledge and research, the issue raised herein was not dealt with or decided and that a similar or identical petition was not filed earlier by them.

10) 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.

CASE IN BRIEF

Centralised Monitoring System (CMS)

11) The Press Information Bureau on November 26th, 2009 in a press release notified the proposal to set up a centralized system to monitor communications on mobile phones, landlines and Internet in the country. The press release described **Centralised Monitoring System ("CMS")** as a 'centralized system to monitor communications on mobile phones, landlines and the Internet in the country which would *"strengthen the security environment in the country".*

Its features included *"Central and regional database that would help Law Enforcement Agencies* **("LEAs")***in the interception and monitoring, and Direct Electronic Provisioning of target numbers by Government agencies without any manual intervention from the Telecom Service Providers* **("TSPs")**, *filters and alert creation on target numbers, Call Data Records* **("CDR")** *analysis and data mining on CDRs to identify call details, location details, etc. of the target numbers and R&D in related fields for continuous upgradation of the speculative profiles of the CMS".* A true copy of the press release dated 26.11.2009 issued by the Press Information Bureau is produced and annexed as **ANNEXURE-P1**(pages 70 to 70).

12) This formed a massive step-forward from the existing surveillance framework, mainly due to its elimination of manual components from the interception chain of command. This automation of the interception established that LEAs using the CMS would no longer need to approach telecom/Internet service providers on a case-by-case basis to retrieve intercepted information as mandated by the Hon'ble Supreme Court in the **People's Union of Civil Liberties (PUCL) v. Union of India &Anr., (1997) 1 SCC 301.**

13) In addition to the content of intercepted communications, the CMS will also have access to communications meta-

data i.e. **Call Detail Records ("CDR")** and **IP Detail Record ("IPDR")**, which will be secured on E1 leased lines through service providers' billing/ mediation servers. A true copy of unstarred question 3207 asked in the Lok Sabha on 12.12.2012 along with the answer is produced and annexed as **ANNEXURE-P2**(pages 71 to 72). A true copy of unstarred question No.1598 asked in the Rajya Sabha on 23.08.2013 along with the answer is produced and annexed as **ANNEXURE-P3**(pages 73 to 74).

14) In 2013, amendments were made to Unified Access Service License ("**UASL**") and Unified License ("**UL**") in order to connect the existing monitoring centres to the CMS network. The said amendments require service providers to provide dark optic fiber connectivity at their own cost up to the nearest point of presence of the CMS network. In case dark optic fiber connectivity is not readily available, (regular) optic fiber connectivity must be provided with 10Mbps bandwidth upgradeable to 45 Mbps when required, but the switch to dark optic fiber was required to be made at the earliest. A true copy of the Amendment made to UASL and UL by the Ministry of Communications and IT Department of Telecommunications (Access Service Cell) File No. 800-12/2013-AS.II dated 14.06.2013 is annexed as **ANNEXURE-P4** (pages 75 to 84).

15) It is submitted that CMS provides direct wiretapping capability for LEAs. Such direct wiretapping leads to an increased surveillance. As per a reply to an RTI application received by the Petitioner No. 2, 7500 to 9000 telephone tapping orders are issued by the Central Government every month. When such a large number of orders are issued by an official periodically, there cannot be an effective application of the mind while scrutinising and issuing them, and also while reviewing them. It is evident from this large number that orders are mechanically issued on the basis of requests made by the LEAs. Ease of conducting telephone tapping and Internet monitoring will only result in the numbers of such tapping /monitoring orders going up. A true copy of the reply to the RTI Application dated 12.05.2014 sent by the Central Public Information Officer (**CPIO**), Ministry of Home affairs is produced and annexed as **ANNEXURE-P5**(pages 85 to 85).

Network Traffic Analysis (NETRA)

16) The Network Traffic Analysis ("**NETRA**") was developed by Centre for Artificial Intelligence ("**CAIR**"), a lab under Defence Research and Development Organization ("**DRDO**") to monitor Internet traffic for the use of keywords such as 'attack', 'bomb', 'blast' or 'kill' in tweets, status updates on social media platforms, emails or blogs. As per reports, NETRA storage servers known as 'nodes'

would be installed at the ISP level at more than 1000 locations across India, each with a storage capacity of 300 GB, thus totalling 300 TB. As per news reports, it can be gathered that **NETRA** will essentially be a dragnet surveillance system designed specifically to monitor the nation's Internet networks including voice over internet traffic passing through software such as Skype or Google Talk, besides write-ups in tweets, status updates, emails, instant messaging transcripts, Internet calls, blogs and forums.

National Intelligence Grid (NATGRID)

17) National Intelligence Grid ("**NATGRID**") is portrayed as an ambitious counter-terrorism initiative to be undertaken on public-private partnership that will utilize technologies like Big Data and analytics to study and analyze huge amounts of data from various intelligence agencies and LEAs to help track suspects and prevent such attacks. It will reportedly collate and analyse data generated by twenty-one (21) standalone databases belonging to various agencies and ministries of the Indian Government, which includes tax and bank account details, credit card transactions, visa and immigration records and itineraries of rail and air travel. This pool of data will then be provided to all security agencies including the Research and Analysis Wing, Intelligence Bureau, the Enforcement

Directorate, the National Investigation Agency, the Central Bureau of Investigation, the Directorate of Revenue Intelligence and the Narcotics Control Bureau. With the use of Big Data and other analytics technologies, NATGRID is also expected to facilitate robust information sharing by various **LEAs**, which will supposedly strengthen their ability to detect terrorist activity, and pre-empt attacks or find the perpetrators.

18) It is submitted that the Petitioner No. 2 filed an application under the Right to Information Act, 2005 seeking information about NATGRID, and in reply from the CPIO (NATGRID) dated 09.06.2011, it is stated that Security agencies can seek the details from the NATGRID database. It is further stated that data from Airline companies, Telecom companies, etc. would be uploaded to NATGRID database. A true copy of the reply dated 09.06.2011 sent by CPIO (NATGRID) is produced and annexed as **ANNEXURE-P6**(pages 86 to 87). However, shortly after this reply was received, NATGRID was placed out of purview of RTI Act, 2005 vide Gazette Notification dated 9.6.2011. A copy of the Gazette Notification dated 09.06.2011 is annexed as **ANNEXURE-P7**(pages 88 to 89).

19) It is submitted that the Ministry of Home Affairs, Cyber and Information Security Division (CIS Division/ CIS-III

Desk), Government of India in its reply dated 27.12.2019 to an RTI question, has confirmed that the NATGRID project has been exempted from the RTI Act, 2005 vide Gazette of India Notification No. GSR 442 (E) dated 09.06.2011 issued by DoP&T. Along with this RTI reply dated 27.12.2019, copies of replies by the Ministry of Home Affairs **(Respondent No. 3)** are annexed which are given in the Parliament with respect to Lok Sabha unstarred question No. 437 for answer on 19.11.2019 and Lok Sabha Unstarred Question No. 881 for answer on 01.03.2016 regarding NATGRID project. Per the response, the NATGRID is expected to be fully rolled out and made operational by 31.12.2020. A true copy of the RTI reply dated 27.12.2019 along with the answers to Lok Sabha unstarred questions No. 437 answered on 19.11.2019 and No. 881 answered on 01.03.2016 is annexed as **ANNEXURE-P8**(pages 90 to 94).

Law Enforcement Agencies (LEAs) Requests for User Data

20) It is submitted that the **LEAs** regularly demand user data from intermediaries like Facebook Inc. and Google Inc. Such requests are on the rise as can be seen from the transparency reports published by these intermediaries. The Transparency Report released by Facebook Inc. shows that between January to June 2019, 22,684 requests for user data were received by Facebook from the Indian Government agencies. These requests are issued under

various statutory provisions like Section 91 of Code of Criminal Procedure 1973 and Section 69 of the Information Technology Act, 2000. A true copy of the relevant pages of Facebook Transparency Report for the period January-June, 2019 is produced herewith and annexed as **ANNEXURE-P9**(pages 95 to 139).

21) It is submitted that the various surveillance mechanisms like **CMS**, **NATGRID** and **NETRA** result in mass surveillance of citizens and arbitrary and excessive monitoring of communication and transactions of users of telecommunication systems.

Pegasus

22) It is submitted that on November 11, 2019, media reports revealed that a malware/spyware named **"Pegasus"** developed by an Israel based cyber intelligence firm "NSO Group Technologies Limited" was used to remotely hack into 1400 WhatsApp accounts and smartphone devices, including 121 Indian users from different backgrounds such as lawyers, human rights activists and journalists. These reports were further confirmed by WhatsApp Inc. when it publicly attributed the attack to NSO Group and filed a complaint against it before the Northern District Court of California for unauthorized use of WhatsApp's servers to install malware/spyware in the targeted victims' devices.

23) It is further submitted that the Citizen Lab, University of Toronto, working in the area of intersection of information and communication technologies, human rights, and global security, published a report titled "Hide And Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries" highlighting that Pegasus was actively used for surveillance in forty five (45) countries, including India. The report further highlighted that the Operator "Ganges" suspected to conduct surveillance in India used a politically themed Internet domain name 'signpetition.co' to insert the spyware in targeted devices. The relevant excerpts of the Citizen Lab Report is annexed as **ANNEXURE-P10**(pages 131 to 149)

24) The Citizen Lab, a Toronto based independent research community has released an article titled "The Dangerous Effects of Unregulated Commercial Spyware" dated 24.06.2019, highlighting a chilling trend observed elsewhere, whereby the political opponents, Human Rights organizations and Lawyers, journalists and members of civic media are disproportionately targeted with powerful spyware technologies, and thereby calling for a an immediate moratorium on the global sale and transfer of the tools of the private surveillance industry until rigorous human rights safeguards are put in place to regulate such practices and guarantee that governments and non-state

actors use the tools in legitimate ways.The relevant excerpts of the Citizen Lab article is annexed as **ANNEXURE - P11**(pages 150 to 154).

25) It is further submitted that NSO Group in response to the media reports stated that **"Pegasus"** was sold only to licensed government intelligence and law enforcement agencies. However, the Hon'ble Union Minister of Electronics and Information Technology has not provided any clear response to the Parliamentary question raised by Hon'ble Member of Parliament Mr. Dayanidhi Maran, regarding the use of Pegasus by the Union Government and/ or LEAs to conduct surveillance on Indian citizens, and/ or any contractual engagements with the NSO Group. Hence, the Union Government's turning down of several requests to provide information on the use of Pegasus raises further doubts about the unlawful and vested use of surveillance machinery without appropriate judicial oversight and procedural safeguards. A true copy of the unstarred question No. 2576 answered on 04.12.2019 is annexed as **ANNEXURE-P12**(pages 155 to 156).

Edward Snowden's Revelations

26) In 2013, Edward Snowden, a former NSA/CIA subcontractor, became a whistle-blower by revealing more than 10,000 documents (later more documents were revealed), which exposed the various mass surveillance

programmes that were operated and executed by the Government of the United States of America, partnering with its allies which had been conducting illegal/secret surveillance even of its own citizens. This revelation triggered a global debate on mass surveillance by the state of its own citizens. The first programme that was revealed under his disclosures is called **"PRISM",** which is the primary data collection programme employed by the United States' NSA which enabled them to collect data from information technology companies such as Microsoft, Yahoo!, Google, Facebook, Paltalk, YouTube, Skype, AOL, and Apple routinely. The data collected includes emails, photos, video and audio chats, Web-browsing content, search engine queries, and all other data stored on their clouds. Another programme employed by the NSA was **"upstream collection"**. Upstream collection was an even more invasive programme. It was employed to capture data directly from private-sector Internet infrastructure - switches and routers that routed Internet traffic worldwide. This meant that almost any person connected to the Internet and used American based services was susceptible to surveillance by the United States. **XKeyscore** is another programme of the NSA, which was already under public knowledge, the Snowden revelations exposed and confirmed which was earlier a secret programme that is used to analyse and search global

Internet data. The Snowden documents also revealed that the United States have shared XKeyscore with the intelligence agencies of Germany, and Japan. The programme is also speculated to have been shared with Australia, New Zealand, Canada, and Britain (under the ***UKUSA Agreement*** for collaboration on signals intelligence, also known as the ***Five Eyes***).

27) A dangerous issue with the **PRISM** programme was that it was backed by court orders wrongly interpreting surveillance law under the US Foreign Intelligence Surveillance Act **("FISA")**. The courts that granted orders allowing for surveillance were secret courts formed under the FISA which gave the NSA grant to conduct surveillance on US citizens. The entire account of the Snowden revelations are not included here due to space constraints. On account of the Snowden revelations, the US had to pass the Freedom Act in 2015 which limited the collection of phone data. The Snowden revelations disclosed that the United States conducted surveillance on citizens of other countries also. Of the countries spied upon, India was among the top targets. A true copy of the article dated 01.02.2014 titled "How Edward Snowden went from loyal NSA contractor to whistle-blower" is produced herewith and annexed as **ANNEXURE-P13**(pages 157 to 169)

28) The Snowden revelations of 2013, created a wave of impact which resonated all over the world. The revelations also resulted in lawsuits in the US such as *ACLU* v. *Clapper* (959 F. Supp. 2d 724, 742 (S.D.N.Y. 2013)), which challenged the NSA's bulk phone metadata collection programme; *Klayman* v. *Obama* (No. 17-5281, United States Court of Appeals for the District of Columbia Circuit) which challenged bulk collection of telephonic and electronic metadata and the PRISM programme; *Rand Paul* v. *Obama* (Civil Action No. 1:14-cv-262-RJL, United States District Court for the District of Columbia) which challenged the US Constitutional validity NSA programmes under the 4th amendment to the US Constitution; and *Wikimedia Foundation* v. *NSA* (1:15-cv-00662-TSE, United States District Court for the District of Maryland) which challenged Upstream surveillance program.

GCHQ Programmes

29) The Snowden Revelations also revealed certain programmes that were being operated by the partners/allies of the NSA such as the Government Communications Headquarters (GCHQ) of the UK Government. The Snowden revelations exposed the existence of **TEMPORA**an earlier secret project that was used by GCHQ to extract Internet communication from

fibre optic cables. The Snowden revelations revealed the fact that the data thus collected was being shared with the NSA. **MUSCULAR** was another programme operated by GCHQ which were exposed by the Snowden revelations. MUSCULAR was used by GCHQ to primarily siphon off data from the internal networks of the Internet companies Yahoo! and Google. This data was also shared with the NSA.

Work by Petitioner No. 2

30) In 2014, Petitioner No. 2 published a report on communications surveillance in India titled **'India's Surveillance State'** describing the procedural and institutional mechanisms of surveillance in India, challenges thereof, advocating for the need of comprehensive surveillance reform in India.

31) The Petitioner No. 2, through research, media reports and several Right to Information applications' replies have understood that there exists a pattern of irregularity, arbitrariness, and surreptitiousness in the execution of **Surveillance Projects** in India and that there is an abuse of process prescribed by laws relevant to surveillance mechanisms. The replies to the RTI applications submitted by Petitioner No. 2 have found that on an average, around 7500 – 9000 telephone-interception orders were being issued by the Central Government alone each month. This was the case during the 2013-2014 period. It is

reasonable to infer that the numbers would have gone up now with increase in connectivity within India over the years.

Puttaswamy (Privacy) Principles and Safeguards

32) That the Hon'ble Supreme Court through a unanimous judgement by 9 Judge Bench in landmark case of ***K. S. Puttaswamyv. Union of India***, (2017) 10 SCC 1 has clarified upon the law related to the right to privacy as a core and basic fundamental right, and constitutes the basic, irreducible condition necessary for the exercise of personal liberty and the freedoms guaranteed by the Constitution. Through the judgment, the Hon'ble Supreme Court recognised that 'informational privacy' is a facet of the right to privacy. Informational privacy enables a person to control the 'dissemination of material that is personal to him.' Unauthorised and illegal surveillance measures is a stab on informational privacy of citizens. The processing of personal data also includes the process of accessing and collecting personal data. The Surveillance Projects illegally accessing and collecting personal data including metadata thwarts the guarantee of the Constitution of India to the people of the right to informational privacy.

33) That the Hon'ble Supreme Court had in **the Puttaswamy (Privacy) judgment** deduced principles which govern the permitted circumstances and requirements when the state

can legally infringe the right to privacy. The principles deduced were *the principle of legitimate state aim; the principle of necessity; the principle of adequacy; and the principle of proportionality.* The Hon'ble Supreme Court held that:

> *"1) There must be a law in existence to justify an encroachment on privacy by the State.*
>
> *2) There must be a legitimate state aim.*
>
> *3) The means which are adopted by the legislature must be proportional to the object and needs of the legislation/provision."*

34) Expanding on the test laid down by Chadrachud, J., Kaul, J. articulated:

> *"The concerns expressed on behalf of the petitioners arising from the possibility of the State infringing the right to privacy can be met by the test suggested for limiting the discretion of the State:*
>
> *(i) The action must be sanctioned by law;*
>
> *(ii) The proposed action must be necessary in a democratic society for a legitimate aim;*
>
> *(iii) The extent of such interference must be proportionate to the need for such interference;*
>
> *(iv) There must be procedural guarantees against abuse of such interference."*

35) Under the principle of legitimate state aim, the communications surveillance should be undertaken only

towards achieving a "predominantly important legal interest that is necessary in a democratic society". The principle of necessity states that communications surveillance may be conducted only when it is the least intrusive means of attaining the legitimate aim. The principle of adequacy states that the choice of specific means of communications surveillance must correspond to the legitimate aim at hand. And the principle of proportionality essentially states that the benefits of communications surveillance should always outweigh its costs.

36) The **principle of legitimate state aim** provides narrowing down the scope of invasive surveillance mechanisms to the direct circumstances, where the very foundations of democratic society are at stake. With the bar set so high, surveillance cannot be undertaken on shaky grounds and in the interest of trifling ends. An examination of the surveillance enabling provisions found across Indian legislations will reveal that communications surveillance is currently permitted on a wide variety of broadly worded grounds, and this includes everything from "protection of national security" to "prevention of spread of computer viruses".

37) The **principle of necessity** requires the employment of the least intrusive means of attaining the legitimate state aim. Strictly speaking, Rule 419A(3) of the Indian

Telegraph Rules 1951 and Rule 8 of the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009 do stipulate that 'other reasonable means' must be considered and exhausted before issuing an interception or monitoring order under the Rules. However, these cautionary provisions are purely procedural hurdles to the actual retrieval of intercepted information. Considering that around 7500 - 9000 phone-interception orders were issued by the Central Government every month (as revealed by an RTI request filed by the 3rd petitioner), careful consideration of less intrusive alternatives in each case would be physically impossible. Further, surveillance systems such as NETRA, which perpetually monitor communication networks call into question the whole premise of Rules 419A and Rule 8 of the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009, since continuous availability of intercepted data would have the effect of dispensing with the very need to resort to other less intrusive means. Also, in the absence of independent oversight, there is no obligation to justify this choice of means. Thus, despite compliant legislative provisions, the principle of necessity is not completely complied in essence.

38) The **principle of adequacy** requires that the mere existence of a legitimate aim must not be grounds for indulging in all kinds of communications surveillance, but the best suited form of surveillance must be identified and employed based on the surrounding circumstances. However, communications surveillance in India is not always conducted in pursuance of a legitimate aim for want of less intrusive alternatives. The nation's communication networks are effectively under perpetual surveillance, with the retrieval of collected information being conditional on the Lea's procurement of a lawful order to do so. Also considering the sheer volume of such lawful orders issued, a case-by-case determination of whether surveillance is the best alternative under the circumstances is almost certainly never done. In the face of such perpetual and unrestricted surveillance, compliance with the principles of legality, necessity, or adequacy looks uncertain.

39) **Proportionality** was another test established in the **Privacy Judgment** to determine the validity of State's interception of citizen's private information. Going by the 'proportionality test', surveillance should only be resorted to following extensive contemplation of the benefits sought to be derived in contrast with the costs associated in the form of compromise of privacy. As much should also be demonstrated before a competent, independent, and

impartial authority, and only once this is done should the actual surveillance be commenced. This is hardly the currently practised model of communications surveillance in India. Surveillance Projects 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.

40) Dragnet surveillance measures are in violation of the three principles as laid down by the Supreme Court in the Privacy Judgment for limiting the right of privacy. With mass surveillance being conducted through the Surveillance projects, the respondents are conducting surveillance excessive of a legitimate state aim for reasons beyond what is prescribed by statutory law; without resorting to 'lesser intrusive means' though 'other reasonable means' are provided for in Rule 419A(3) of the Indian Telegraph Rules 1951 and Rule 8 of the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009; indulging in blanket monitoring of all communication systems without resorting to a specific choice of communication surveillance; and disproportionately without judicial oversight.

41) That, the procedural safeguards and interception standards for NATGRID, its governing laws to prevent the leak or misuse of collated data, despite being of critical importance, have not been disclosed by the Respondent-State and cannot be availed for public scrutiny as questions asked under the Right to Information Act, 2005 are denied answers citing exemption under Section 8 of the Act.

42) That, the collection and aggregation of metadata of an individual's various transactions including communication, financial and travel information will result in a real time profiling of the entire population. There is no law governing such profiling and the entire population is at the mercy of the Government. The surveillance in the case of NATGRID affects the entire population and is pervasive. Such a pervasive surveillance is illegal and infringes the fundamental right to privacy, undertaken without any enabling law.

43) That, the collection and analysis of metadata without obtaining consent and on a massive scale without judicial oversight violates the reasonable expectation of privacy of citizens as metadata could be used to reveal information such as civil, political, religious affiliation, social status, support to a charitable organization, and subject's involvement in an intimate relationship. Ergo, the more metadata government collects and analyses, the greater

the capacity for such metadata to reveal more private previously unascertainable information about individuals.

44) That, such methods of data collection have innumerable implications, including an impact on decision-making of an individual and imposing a chilling effect on the right to free speech. Justice Bobde shared a very interesting insight on the same in the **Puttaswamy (Privacy) Judgment**, where he held, in Para 22, Page no. 19, that:

> *"Every individual is entitled to perform his actions in private. In other words, she is entitled to be in a state of repose and to work without being disturbed, or otherwise observed or spied upon. The entitlement to such a condition is not confined only to intimate spaces such as the bedroom or the washroom but goes with a person wherever he is, even in a public place. Privacy has a deep affinity with seclusion (of our physical persons and things) as well as such ideas as repose, solitude, confidentiality and secrecy (in our communications), and intimacy. But this is not to suggest that solitude is always essential to privacy. It is in this sense of an individual's liberty to do things privately that a group of individuals, however large, is entitled to seclude itself from others and be private. In fact, a conglomeration of individuals in a space to which the rights of admission are reserved – as in a hotel or a cinema hall –must be regarded as private. Nor is the*

right to privacy lost when a person moves about in public. The law requires a specific authorization for search of a person even where there is suspicion. Privacy must also mean the effective guarantee of a zone of internal freedom in which to think."

45) That, aside from judicial pronouncements, right to privacy in India is also influenced by **the Universal Declaration on Human Rights ("UDHR")** and **the International Covenant on Civil and Political Rights ("ICCPR")**, both of which recognize the individual's right to privacy. In addition, Article 51 of the Constitution of India directs that the State shall endeavour to inter alia, foster respect for international law and treaty obligations in the dealings of organised peoples with one another. Article 17.1 of the International Covenant on Civil and Political Rights, 1966, to which India is a State Party states that:

***"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."*

(emphasis added)

46) That the Hon'ble Supreme Court has time and again pointed out to the observance of international obligation that India has in various domains. Also, the Universal Declaration of Human Rights, 1948, which is a

foundational document for international human rights treaties, states, in its Article 12,

> ***"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence,*** *nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."*
>
> (emphasis added)

47) That, General Comment No. 16 (1988) by the Center for Civil and Political Rights("CCPR"), adopted by the Human Rights Council ("HRC") of the United Nations ("UN") said surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations, should be prohibited. It also indicated that the gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. In its General Comment No. 34 (2011), the HRC analysed the relationship between the Right to Freedom of Expression and Opinion and the Right to Privacy, underlining how the latter is often an essential requirement for the realization of the latter.

48) That, **the Resolution on Right to Privacy in the Digital Age** adopted by the UN General Assembly calls upon its members

'to review their procedures, practices and legislation regarding the surveillance of communications, their interception and 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'.

49) That the Resolution on Right to Privacy in the Digital Age notes that new technologies that increase the ability for surveillance, interception and data collection by governments, companies and individuals may violate or abuse human rights, in particular the right to privacy. The adoption of this Resolution is a milestone since the General Assembly has established, for the first time, that human rights should prevail irrespective of the medium and therefore need to be protected both off-line and on-line. Further, the General Assembly had, in its above-mentioned Resolution on Right to Privacy in the Digital Age, asked the UN High Commissioner on Human Rights ("HCHR") to submit a report ("Report") on the protection and promotion of the right to privacy in the context of domestic and extraterritorial surveillance and/or the interception of digital communications and the collection of personal data, including on a mass scale, to the Human Rights Council at its 27th session and to the General

Assembly at its 69th session. With regard to surveillance and collection of personal data, the Report concludes that practices in many States reveal a lack of adequate national legislation and/or enforcement, weak procedural safeguards and ineffective oversight, all of which contribute to a lack of accountability for arbitrary or unlawful interference in the right to privacy. As an immediate measure, the Report suggests that States review their own national laws, policies and practices to ensure full conformity with international human rights law.

50) That, the Surveillance Projects and projects that employ the use of malware/spyware such as Pegasus, in effect, do away with manual processing of requests and orders to conduct surveillance. While the interception process under the CMS is claimed to be governed by the procedure laid down by Section 5 of the Indian Telegraph Act, 1855 read with Rule 419A of the Indian Telegraph Rules, 1951, the fact that the CMS is capable of Direct Electronic Provisioning of target numbers runs foul of said procedures since it dispenses with the chain of command involving manual elements such as nodal officers meant to authorize interception requests. These mechanisms are prone to abuse and can be used to target non-threats to national security such as lawyers, human rights activists, social workers, journalists etc. This fact is already being

established with the exposure of malware/spyware such as Pegasus. This results in large scale dragnet surveillance of users without any judicial oversight which is illegal and a threat to the rights guaranteed under the Constitution of India.

51) **That, the need of a robust independent oversight mechanism in the form of Judicial and/or Parliamentary Authority is a necessary check against unlawful surveillance in a democratic society.** The Right to Privacy is prima facie violated by India's communications surveillance framework for the simple reason that there is absolutely no judicial intervention and oversight at any stage of the surveillance process. No provisions of law as they currently stand, talk about judicial oversight in any capacity. Thus, it is important to have judicial oversight for any order imposing surveillance. An important parallel that can be drawn is the provisions as to search and seizure of documents that are provided for in the Code of Criminal Procedure, 1973 under Sections 93, 94, 97, and 98, show that in order for law enforcement agencies to violate the privacy of an individual and seize incriminating documents or items, a warrant of a court of law is mandatory. A parallel may also be drawn from the Fourth Amendment to the Constitution of the United States wherein it is stated that:

"The right of the people to be secure in their persons, houses, papers, and effects,(a) against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

However, it is startling to see that dragnet and mass surveillance are being executed on Indian citizens through the Surveillance projects bypassing judicial scrutiny and review, collecting and aggregating information that can be used to incriminate individuals before a court of law.

52) That, though the Indian Telegraph Rules 1951 and the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009 provide for the establishment of a Review Committee towards reviewing surveillance directives. The 2009 IT Rules imports the definition of the Review Committee established in Rule 419A of the Telegraph Rules, 1951. The respondent No. 2 vide Gazette notification dated 24.02.2014 amended Rule 419A of Indian Telegraph Rules, 1951.This Committee is comprised solely of members of the executive branch of the Government.

Rule 419A sub-rule (16) states:

"(16) The Central Government and the State Government, as the case may be, shall constitute a Review Committee. The Review Committee to be constituted by the Central Government shall consist of the following, namely:

1. Cabinet Secretary — Chairman

2. Secretary to the Government of India Incharge, Legal Affairs — Member

3. Secretary to the Government of India, Department of Telecommunications — Member

The Review Committee to be constituted by a State Government shall consist of the following, namely:

1. Chief Secretary — Chairman

2. Secretary Law/Legal Remembrancer Incharge, Legal Affairs — Member

3. Secretary to the State Government (other than the Home Secretary) — Member"

When provisions of law stipulate systematic review of any activity capable of causing harm in the absence of oversight, it logically follows that fairness of review cannot be guaranteed in the presence of conflicting interests. If those undertaking and reviewing such potentially harmful activity belong to the same broad vehicle of the Government, conflicting interests are all but unavoidable and this leads to a complete breakdown of the review process itself. The Hon'ble Supreme Court

in the Privacy Judgement has held that there should be application of judicial mind when the state infringes the fundamental right to privacy under any combination of the Articles 14, 19(1)(a), and/or 21 of the Constitution of India. Relevant extract from the Privacy judgement reported as (2017) 10 SCC 1, is reproduced hereinbelow:

"*526. But this is not to say that such a right is absolute. This right is subject to reasonable regulations made by the State to protect legitimate State interests or public interest. However, when it comes to restrictions on this right, the drill of various articles to which the right relates must be scrupulously followed. For example, if the restraint on privacy is over fundamental personal choices that an individual is to make, State action can be restrained under Article 21 read with Article 14 if it is arbitrary and unreasonable; and under Article 21 read with Article 19(1)(a) only if it relates to the subjects mentioned in Article 19(2) and the tests laid down by this Court for such legislation or subordinate legislation to pass muster under the said article. Each of the tests evolved by this Court, qua legislation or executive action, under Article 21 read with Article 14; or Article 21 read with Article 19(1)(a) in the aforesaid examples must be met in order that State action pass muster. In the ultimate analysis, the balancing act that is to be carried out between individual, societal*

and State interests must be left to the training and expertise of the judicial mind."

53) That the Respondent No. 2 in its reply letter dated 08.01.2020 to an RTI query affirmed that the **CMS** project is currently operational, and its functioning along with the applicable safeguards for preventing misuse of data collected through CMS is as under Rule 419-A of the Indian Telegraph Rules 1951. This confirms the inadequate safeguards in the legal framework of issuing and reviewing interception orders and also does not meet the proportionality standards as laid down by the Hon'ble Supreme Court in ***Puttaswamy*** (Privacy-9J) judgement. A true copy of the RTI reply dated 08.01.2020 along with the Gazette Notification amending Rule 419(A) of Indian Telegraph Rules 1951 dated 24.02.2014 is produced herewith and annexed as **ANNEXURE - P14**(pages to 170).

54) That, currently, there exist no provisions of law whereby users are notified when their communications are subjected to surveillance, and no distinction is made between situations where such notification would defeat the purpose of surveillance and otherwise. By extension, users also lack the ability to appeal the decision to conduct surveillance of their communications. Even once active surveillance has been concluded, collected information is retained for specified periods after which

they are required to be destroyed, all without intimating the user. Thus, it is entirely possible in the present scenario for the bulk of a users' communications to be subjected to extensive surveillance leaving him/her completely unaware.

55) The importance of having an independent oversight mechanism has been stressed upon and covered in detail in the Report dated 27.07.2018 submitted by the Committee of Experts under the Chairmanship of Justice B N Srikrishna, Former Judge, Supreme Court constituted by the Government of India to identify, deliberate, andsuggest data protection issues and legal framework. The relevant text from the Report is extracted hereinbelow:

"Surveillance should not be carried out without a degree of transparency that can pass the muster of the Puttaswamy test of necessity, proportionality and due process. This can take various forms, including information provided to the public, legislative oversight, executive and administrative oversight and judicial oversight. This would ensure scrutiny over the working of such agencies and infuse public accountability. Executive review alone is not in tandem with comparative models in democratic nations which either provide for legislative oversight, judicial approval or both. Legislative oversight exists in Germany; judicial review in UK; and some form of both in South Africa. At the same time, it is instructive to note that the data protection

legislations in each of these countries dovetail with each substantive legislation relating to national security. Thus, in South Africa, under the Intelligence Services Oversight Act, 1994 there is a parliamentary as well as civil oversight mechanism which together hold security structures accountable and receives complaints about intelligence services.

....

Nothing similar exists in India. This is not just a gap that is deleterious in practice but, post the judgment of the Supreme Court in Puttaswamy, potentially unconstitutional. This is because the Supreme Court has clearly laid down that any restriction of the right to privacy must satisfy three tests; first, the restriction must be by law, second, it must be necessary and proportionate and third, it must promote a legitimate state interest. The salience of procedural safeguards within the interception structure has also been emphasised to prevent abuse."

56) The European Court of Human Rights (ECtHR) has recently observed in its judgement dated 13.09.2018 in case of *BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM* (Applications nos. 58170/13, 62322/14 and 24960/15)about the necessity of a robust independent oversight mechanism in a democratic society to balance and protect the interests of the State and of the

individual's right to privacy. Extracting relevant text from the judgement below:

"308. As to the question whether an interference was "necessary in a democratic society" in pursuit of a legitimate aim, the Court has acknowledged that, when balancing the interest of the respondent State in protecting its national security through secret surveillance measures against the seriousness of the interference with an applicant's right to respect for his or her private life, the national authorities enjoy a certain margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security. However, this margin is subject to European supervision embracing both legislation and decisions applying it. In view of the risk that a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there are adequate and effective guarantees against abuse. The assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law. The Court has to determine whether the procedures for supervising the ordering and implementation of the restrictive measures are such as to keep the "interference"

to what is "necessary in a democratic society" (see Roman Zakharov, cited above, § 232; see also Klass and Others v. Germany, 6 September 1978, §§ 49, 50 and 59, Series A no. 28, Weber and Saravia, cited above, § 106 and Kennedy, cited above, §§ 153 and 154).

...

346. [I]n a bulk interception regime, where the discretion to intercept is not significantly curtailed by the terms of the warrant, the safeguards applicable at the filtering and selecting for examination stage must necessarily be more robust.

347. Therefore, while there is no evidence to suggest that the intelligence services are abusing their powers – on the contrary, the Interception of Communications Commissioner observed that the selection procedure was carefully and conscientiously undertaken by analysts (see paragraph 179 above) –, the Court is not persuaded that the safeguards governing the selection of bearers for interception and the selection of intercepted material for examination are sufficiently robust to provide adequate guarantees against abuse. Of greatest concern, however, is the absence of robust independent oversight of the selectors and search criteria used to filter intercepted communications."

GROUNDS

A) Because the Surveillance Projects effectuating a massive, illegal dragnet surveillance of Telecom and Internet communications of Indian citizens in bulk violates the fundamental right to privacy under Articles 19(1)(a) and 21 of the Constitution, as law laid down by the Hon'ble Supreme Court in the Privacy Judgement.

B) Because the Surveillance Projects does not follow the privacy safeguards with adequate oversight as laid down by the Hon'ble Supreme Court in the*PUCL vs. Union of India (1997) AIR 568* and in *K. S. Puttaswamy vs. Union of India (Privacy) (2017) 10 SCC 1.*

C) Because the aggregation of metadata of an individual's various transactions including financial and travel information will result in a real time profiling of the entire population, and could be used to reveal information such as civil, political, religious affiliation, social status, support to a charitable organization, and subject's involvement in an intimate relationship. Such methods of data collection have innumerable implications, including an impact on decision-making of an individual and imposing a chilling effect on right to free speech thereby restricting the fundamental right to speech and expression under Art. 19(1)(a). Ergo, the more metadata government collects and analyses, the greater the capacity for such metadata to reveal more private

previously unascertainable information about individuals.

D) Because India is a Party to the International Covenant on Civil and Political Rights ("ICCPR") and has voted in favour of the Universal Declaration of Human Rights ("UDHR"), both of which recognize the individual's right to privacy. In addition, Article 51 of the Constitution of India directs that the State shall endeavour to inter alia, foster respect for international law and treaty obligations in the dealings of organised peoples with one another.

E) Because the Surveillance Projects and programmes that employs the use of malware/spyware such as Pegasus, in effect, do away with manual processing of requests and orders to conduct surveillance and interception. While the interception process under the CMS is claimed to be governed by the procedure laid down by Section 5 of the Indian Telegraph Act, 1855 read with Rule 419A of the Indian Telegraph Rules, 1951, the fact that the CMS is capable of Direct Electronic Provisioning of target numbers runs afoul of said procedures since it dispenses with the chain of command involving manual elements such as nodal officers meant to authorize interception requests.

F) Because the need of a competent judicial authority is a necessary check against unlawful surveillance. The Right to Privacy is prima facie violated by India's

communications surveillance framework for the simple reason that there is absolutely no judicial intervention at any stage of the surveillance process. The Indian Telegraph Rules 1951 and the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009 provide for the establishment of a Review Committee towards reviewing surveillance directives comprised solely of members from the executive branch of the Government.

G) Because, the Surveillance Projects namely "CMS", "NETRA", and "NATGRID" are ultra vires to Articles 14, 19(1)(a) and 21 of the Constitution of India. The right to privacy is embedded into the Constitution of India in Part III, primarily under the aforementioned Articles and its essence can be deduced in other rights in Part III. The Surveillance projects which conduct unbridled collection, processing, and storage of massive personal data violates the basic and fundamental right to privacy under the Constitution and the law laid down by the Hon'ble Supreme Court in the K.S. Puttaswamy (Privacy) judgment.

57) That this Hon'ble High Court has jurisdiction to decide the matter as all the Respondents arepublic authorities as per Article 12 of the Constitution of India, and are located within Delhi and so comes under the jurisdiction of the Delhi High Court.

58) The Petitioners therefore, most humbly submit that it would be just, expedient and in the interest of justice that this Hon'ble High Court be pleased to grant the Petitioners following prayers and also the interim reliefs sought by the Petitioners pending the hearing and final disposal of this Petition.

59) The petitioners have not filed any other similar writ petition regarding the matter in dispute before the Hon'ble Supreme Court or any other High Court.

60) That the annexures appended to the petition are true copies of their respective originals which they pertain to be so.

PRAYERS

In the light of the facts and circumstances stated hereinabove, it is most humbly requested that this Hon'ble High Court may be pleased to:

A. Issue a writ of Mandamus or any other appropriate writ, order or direction directing the respondents to permanently stop the execution and the operation of the **Surveillance Projects** namely "CMS", "NETRA", and "NATGRID" which allows for bulk collection and analysis of personal data;

B. Issue a writ of Mandamus or any other appropriate writ or order directing the respondents to constitute and

establish a permanent independent oversight body – Judicial and/or parliamentary body, for issuing and reviewing lawful interception and monitoring orders/ warrants under the enabling provisions of Indian Telegraph Act, 1885 and the Information Technology Act, 2000;

C. Pass such other order as this Hon'ble High Court may deem fit and proper in the facts and circumstances of the case.

Paiswal

THROUGH:

Prashant Bhushan

(PRASHANT BHUSHAN)

COUNSEL FOR THE PETITIONERS

DRAWN BY:

HEMANTH POTHULA, ADVOCATE
PRASANTH SUGATHAN, ADVOCATE
BASIL AJITH, ADVOCATE

DRAWN AND FILED ON: 28.02.2020
PLACE: NEW DELHI