IN THE HIGH COURT OF DELHI AT NEW DELHI

WRIT PETITION (C) No. 8998 OF 2020

IN THE MATTER OF:

CENTRE FOR PIL AND ANR. .....PETITIONERS

Versus

UNION OF INDIA & ORS.
.....RESPONDENTS

N.D.O.H.: 07.01.2021

I N D E X

Sl. No.	**Particulars**	**Page Nos.**
1.	SHORT AFFIDAVIT ON BEHALF OF THE RESPONDENTS No. 2, 3 & 4	1-15
2.	**Annexure-A** Copy of the text containing the Rules so framed in exercise of the said powers being Information Technology [Procedure and Safeguards for Interception, Monitoring and Decryption of Information] Rules, 2009, and Rule 419A of Indian Telegraph Rules.	16 - 24

RESPONDENT NO. 2, 3 & 4

Through

(AJAY DIGPAUL)
Central Government Standing Counsel
Chamber No. 138-139, Patiala House courts,
New Delhi-110001.
Mobile-9811157265
Email: digpaulassociates@yahoo.co.in

Date: 05/01/2021
Place: New Delhi.

(1)

IN THE HIGH COURT OF DELHI AT NEW DELHI

WRIT PETITION (C) No. 8998 OF 2020

IN THE MATTER OF:

CENTRE FOR PIL AND ANR. .....PETITIONERS

Versus

UNION OF INDIA & ORS.

.....RESPONDENTS

SHORT AFFIDAVIT ON BEHALF OF RESPONDENTS NO. 2, 3 & 4.

I, Rakesh Kumar, presently working as Under Secretary to the Government of India in the office of Ministry of Home Affairs, North Block, New Delhi, do hereby solemnly affirm and state as under :-

1. That I am authorized in my official capacity to swear and depose to the present affidavit and as such, I am aware of the facts and circumstances based on the records of the case.

2. That the present Reply/Short Affidavit to deal with the main challenges raised in the captured petition regarding constitutional validity of section 5(2) of the Indian Telegraph Act and section 69 of Information Technology Act, and functioning of NATGRID, Centralized Monitoring System (CMS) and NETRA for lawful interception and monitoring by law enforcement agencies, is being filed by

(राकेश कुमार)
(RAKESH KUMAR)
अवर सचिव
Under Secretary
गृह मंत्रालय
Ministry of Home Affairs
भारत सरकार, नई दिल्ली
Govt. of India, New Delhi

the answering respondent on the basis of inputs submitted by the respondent nos. 2, 3 & 4, without dealing with the petition para-wise. Unless any averment is not specifically admitted, the same may be treated as denied.

3. That as far as prayer sought by the petitioner whereby directing the respondents to permanently stop the execution and the operation of the alleged Surveillance Projects namely "CMS", "NETRA", and "NATGRID" which allows for bulk collection and analysis of personal data and 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 is concerned, the answering Respondent herein vehemently denies the allegations and claims made in the petition and it is submitted that the petitioner has based his petition mostly on factually and technically inaccurate knowledge that he gathered from his unconfirmed sources. At the outset, it is submitted that Lawful Interception or monitoring or decryption of any message or class of messages or any information stored in any computer resources, is done by authorized law enforcement agencies having legal and statutory powers and after due approval of each case by the competent authority, as per the legal provisions contained in section 5 (2) of the Indian

Telegraph Act, 1885 read with Rule 419-A of the Indian Telegraph Rules, 1951 and Section 69 of the Information Technology Act, 2000 read with The Information Technology (Procedure and safeguards for Interception, Monitoring and Decryption of information) Rules, 2009 and as subject to safeguards as provided in the prescribed rules and SOP.

4. The safeguards and review mechanism have been prescribed in the Rule 419A of the Indian Telegraph Rules; and the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 and Standard Operating Procedure issued for the purpose. There is no blanket permission to any agency for interception or monitoring or decryption; and permission from competent authority is required, as per due process of law and rules in each case. Provisions contained in section 69 of the Information Technology Act, 2000 provides power to the competent authority for interception and monitoring and it is read as under:-

> "**69. Power to issue directions for interception or monitoring or decryption of any information through any computer resource**
>
> *(1) Where the Government or a State Government or any of its of specially authorized by the Central Government of the State Government, as the case may*

(RAKESH KUMAR)
Under Secretary
Ministry of Home Affairs
Govt. of India, New Delhi

The Seal of Oath Commissioner
Sl. No. 7305
NEELAM SHARMA
Addl. Govt. of NCT of Delhi
New Delhi

be, in this behalf may, if satisfied that it is necessary or expedient to do in the interest of the sovereignty or integrity of India, defense of India, security of the state, friendly relation with the foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may, subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource.

(2) The procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed.

(3) The subscriber or intermediary or any person in-charge of the computer resource shall, when called upon by any agency referred the in sub-section (1), extend all facilities and technical assistance to–

a) Provide access to or secure access to the computer resource generating, transmitting, receiving or storing such information; or

b) Intercept, monitor, or decrypt the information, as the case may be; or

c) Provide information stored in computer resource.

(4) The subscriber or intermediary or any person who fails to assist the agency referred to in sub-section (3) shall be punished with imprisonment for a term which may extend to seven years and shall also be liable to fine.'

(RAKESH KUMAR)
Under Secretary
Ministry of Home Affairs
Govt. of India, New Delhi

Seal of Oath Com... Sl. No. 7905 ... New Delhi

5. That similarly the power existed in the competent authority under section 5(2) of the Indian Telegraph Act, 1885 which is reproduced hereunder:-.

Section 5(2) in The Indian Telegraph Act, 1885

"On the occurrence of any public emergency, or in the interest of the public safety, the Central Government or a State Government or any officer specially authorised in this behalf by the Central Government or a State Government may, if satisfied that it is necessary or expedient so to do in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of an offence, for reasons to be recorded in writing, by order, direct that any message or class of messages to or from any person or class of persons, or relating to any particular subject, brought for transmission by or transmitted or received by any telegraph, shall not be transmitted, or shall be intercepted or detained, or shall be disclosed to the Government making the order or an officer thereof mentioned in the order: Provided that the press messages intended to be published in India of correspondents accredited to the Central Government or a State Government shall not be intercepted or detained, unless their transmission has been prohibited under this sub-section."

(RAKESH KUMAR)
Under Secretary
Ministry of Home Affairs
Govt. of India, New Delhi

6. That the Section 69 of the Information Technology Act,2000 and section 5(2) of the Indian Telegraph Act, 1885 itself mandates self-contained safeguards to ensure that fundamental rights of any citizen either under Article 19(1)(a) or otherwise, is not adversely affected. The

The Seal of Oath Commissioner * New Delhi *
Sl. No. 7305
NEELAM SHARMA
Advocate Govt. of NCT of Delhi

permissible purposes for which power under the Act can be exercised, necessarily are those having legitimate State interest and larger public interest. In other words, the exercise of powers under the Act is permissible only for statutorily specified and precisely defined purposes mentioned in the said provision and not otherwise.Such safeguards are mandated to be provided for by way of a delegated legislation namely by making statutory rules. A copy of the text containing the Rules so framed in exercise of the said powers being Information Technology [Procedure and Safeguards for Interception, Monitoring and Decryption of Information] Rules, 2009, and Rule 419A of Indian Telegraph Rules, are annexed herewith as **Annexure-A**.

7. That it is respectfully stated and submitted that there is no blanket permission to any agency for interception or monitoring or decryption as the authorized agencies require permission of the competent authority i.e. Union Home Secretary in each case as per due process of law and justification for interception or monitoring or decryption. It is further submitted that such a permission can be given only for the purposes mentioned in the section 69 of the IT Act 2000, i.e. sovereignty and integrity of India, defense of India, security of the State, friendly relations with foreign States, public order, preventing incitement to the commission of any cognizable offence relating to above, or investigation of any offence. Further, the SOP for interception, handling, Use, Copying, Storage and Destruction of Messages /telephonic intercept/emails under section 5(2) of Telegraph Act and section69 of IT Act issued by MHA on 19.5.2011, clearly mandates that the direction for interception or monitoring of any message or class of messages or any information generated, transmitted, received or stored in any computer resource shall be issued

(RAKESH KUMAR)
Under Secretary
Ministry of Home Affairs
Govt. of India, New Delhi

The Seal of Oath
Sl. No. 7305
NEELAM SHARMA
Advocate
Regd. of Oath
New Delhi

(7)

by the competent authority. Detailed process has been laid for security and law enforcement agencies also which inter-alia includes that request for interception or monitoring shall be made by the Head of authorized security or law enforcement agency. Further, it is also mandated in the SOP that any proposal for interception or monitoring shall be made after considering the possibility of acquiring necessary information by other means; and that the proposal shall be made only when it is not possible to acquire the information by any other reasonable means.

8. That the contentions of the petitioner that the interception orders are mechanically issued on the basis of requests made by the LEAs are totally wrong and hence, vehemently denied. In this regard, it is respectfully submitted that every proposal received from authorized law enforcement agencies for interception and monitoring, are scrutinized by the dedicated Unit of the Ministry of Home Affairs with strict security and confidentiality before consideration by the Union Home Secretary as competent authority at Central Government, for the approval of proposal as per legal provisions contained in section 69 of the Information Technology Act, 2000 and section 5(2) of the Indian Telegraph Act, 1885.

9. That it is submitted that sufficient mechanism of oversight is in place under Rule 419A of Indian Telegraph Rules and IT (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009 as per directions issued by the Hon'ble Supreme Court in People's Union for civil Liberties (PUCL) v. Union of India [1997(1) 8CC 301]. Rule 419A of Indian Telegraph Rules adequately provides that the Central Government and the State Government, as the case may be, shall constitute a Review Committee. The Review Committee constituted by the Central Government,

(RAKESH KUMAR)
Under Secretary
to the Govt. of India
Ministry of Home Affairs
Govt. of India, New Delhi

shall consist of Cabinet Secretary as Chairman, Secretary to the Government of India (In charge of Legal Affairs), Secretary to the Government of India (Department of Telecommunications) as members and the Review Committee constituted by the State Government shall consist of Chief Secretary as Chairman, Secretary Law/ Legal Remembrance and Secretary to the State Government (other than the Home Secretary) as members. The Rule also provides for mandatory forwarding of interception order to the concerned Review Committee. The Review Committee within period of sixty days from the issue of the directions shall *suo moto* make necessary enquiries and investigations and record its findings whether the directions issued by the competent authority, are in accordance with the provisions of Section 69 of the Information Technology Act 2000 or Section 5(2) of the India Telegraph Act. When the Review Committee is of the opinion that the directions are not in accordance with the provisions referred to above, it may set aside the directions and order for destruction of the copies of the intercepted, message or class of messages.

10. That answering respondent respectfully submits that the Review Committee headed by the Cabinet Secretary is competent to review each case of interception and issue directions to set aside any direction for interception and also order for destruction of the copy of intercepted message or class, of message. One of the members of the Committee is the Secretary In-charge of Legal affairs, who also applies his judicial mind as a member of the committee and contributes in that respect also in the judicious review of the directions issued under the act. Further, Article 32 of the constitution also provides for judicial review of the executive actions. Therefore, the existing safeguards of oversight by high level committee chaired by the Cabinet

(राकेश कुमार)
(RAKESH KUMAR)
अवर सचिव
Under Secretary
गृह मंत्रालय
Ministry of Home Affairs
भारत सरकार
Govt. of India, New Delhi

(9)

Secretary at Central level and chaired by Chief Secretary at State level, are adequate and provide effective supervision. It is therefore evident that comprehensive guidelines and SOP have been issued to provide safeguards; and the need to follow it, has also been reiterated to enforcement / security agencies from time to time.

11. That the records pertaining to such directions for interception and of intercepted messages shall be destroyed by the relevant competent authority and the authorized security and Law Enforcement Agencies every six months unless these are, or likely to be required for functional requirement.

12. That it is further submitted that the Right to privacy is a very important right. The impugned provisions are justified on the basis of a law which stipulates a procedure which is fair, just and reasonable and that any invasion of any right is met by the three-fold requirement of (i) legality; (ii) need; and (iii) proportionality, which means that:

i. The action must be sanctioned by law;

ii. The proposed action must be necessary 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.

13. That the answering respondent respectfully submits that the Section 69 of the IT Act 2000 and section 5(2) of Telegraph Act meets the aforesaid requirements and Rules made thereunder further ensure that no fundamental right

(RAKESH KUMAR)
Under Secretary
Ministry of Home Affairs
Govt. of India, New Delhi

The Seal of Office
New Delhi

including the right to privacy of law abiding citizens is violated by any agency, intermediary or person.

14. That further the Article 14 of the constitution of India provides that the State shall not deny to any person equality before the' law or equal protection of the laws within the territory of India. The provisions of section 69 of the Information Technology Act, 2000 and section 5(2) of telegraph Act are equally applicable to all persons as per provisions of law, which are just fair and reasonable; and subject to the safeguards provided by law and procedure established under the law.

15. It is further submitted that the grave threats to the country from terrorism, radicalization, cross border terrorism, cybercrime' organized crime, drug cartels cannot be understated or ignored and a strong and robust mechanism for timely and speedy collection of actionable intelligence including digital intelligence, is imperative to counter threats to national security. This is undeniably legitimate State interest. It is therefore imperative that the requests for lawful interception monitoring must be dealt with by the executive authority to maintain speed and promptitude in taking decisions. A well laid down procedure for oversight by a committee headed by the Cabinet Secretary doubtlessly ensures that the provisions of law, rules and SOP are adhered to.

(राकेश कुमार)
(RAKESH KUMAR)
अवर सचिव
Under Secretary
Ministry of Home Affairs
Govt. of India, New Delhi

16. It is further submitted that though the right to privacy is held to be a sacred fundamental right and is being respected by the Government of India, the veil of privacy can be lifted for legitimate State interest namely in the interest of sovereignty or integrity of India, defense of India, security of the State, friendly relations with foreign States or public order or for, preventing incitement to the

Seal of Oath Commissioner
Sl. No. 7305
NEELAM SHARMA

(11)

commission of any cognizable offence relating to the above referred categories or for investigation of any offence. All the aforesaid categories fall within the "legitimate State interest" making exercise of the power under aforementioned sections permissible when violating or infringing upon the right to privacy as all the aforesaid factors are factors in furtherance of legitimate State interest.

17. That the contentions of the petitioner that Centralized Monitoring System (CMS), NATGRID and NETRA allow the law enforcement agencies for bulk collection and analysis of personal data illegally and do not follow the privacy safeguards with adequate oversight as laid down by the Hon'ble Court, are totally wrong and denied. It is respectfully submitted that the structure and functioning of CMS, NATGRID and NETRA, are designed to strengthen the existing lawful interception process for more secure and transparent functional within prescribed legal provisions and procedures as explained in the above paras.

18. **The Centralized Monitoring System (CMS)** facilitates to automate provisioning of interception order issued under Section 5(2) of Indian Telegraph Act or Section 69 of Information Technology Act, for the Lawful Interception and Monitoring and ensures secured delivery of intercepted content to the authorized law enforcement agency concerned. CMS is a system which allows fast and immediate electronic provisioning of targets for lawful interception without manual intervention of Telecom Service Providers (TSPs). The system is designed to have inbuilt checks and balances wherein Law Enforcement Agencies (LEAs) cannot provision the interception directly. Interception is provisioned by the Telegraph Authority at

(राकेश कुमार)
(RAKESH KUMAR)
अवर सचिव
Under Secretary
गृह मंत्रालय
Ministry of Home Affairs
भारत सरकार
Govt. of India, New Delhi

RMC (Regional Monitoring Centre) after ensuring that there are proper approvals and authorization by the competent authority and Telegraph Authority cannot see the content of intercepted communications. Review Committee under the Chairmanship of Cabinet/Chief Secretary of the respective states, as the case may be, are required to review the cases of interception once in 2 months. The storage and destruction of the intercepted data is as per Rule 419(A) of Indian Telegraph Rules.

19. It is absolutely incorrect to say that CMS allows LEAs to bypass the existing procedural safeguards, instead it strengthens the safeguards. A level of check is introduced at the level of Telegraph Authority to verify that all the interceptions being carried out by LEAs have the due approvals. It strengthens the check and balance mechanism, while expediting the receipt of authorized intercepted information by the LEAs. CMS system does not store/analyze the intercepted data.

20. That the answering respondent further submits that the **NATGRID** is portrayed as an ambitious counter-terrorism initiative to be undertaken on a public-private partnership. This contention of the petitioner is denied and it is respectfully clarified that NATGRID is established as an attached office of Ministry of Home Affairs vide a decision of the CCS. As against the contentions of petitioners, it is submitted that, NATGRID project does not result in real-time profiling of individuals, per se. It only facilitates User Agencies (UAs) to seek and analyse information on selective

(राकेश कुमार)
(RAKESH KUMAR)
अवर सचिव
Under Secretary
Ministry of Home Affairs
गृह मंत्रालय
Govt. of India, New Delhi

Seal of Oath Commissioner

entities so as to identify suspects that pose potential threat to national and internal security.

21. That the NATGRID's IT platform has been envisaged as an anti-terror framework to facilitate access of information on selective entities from various data sources who are its Providing Organizations (POs) in a timely and secure manner, and present an integrated view of terror related information to its User Agencies (UAs)making use of technologies and analytics. NATGRID's mandate is to facilitate collection of information by UAs within their respective legal mandates e.g. Code of Criminal Procedure, 1973, Prevention of Money Laundering Act, 2002, Information Technology Act etc. It is also to bring into the notice of this Court that NATGRID is not involved in monitoring of communications or transactions of users of tele communication system as alleged by the petitioners. It only facilitates UAs to seek and analyse information on selective entities so as to identify suspects that pose potential threat to national and internal security.

22. That it is further submitted that similarly, **NETRA** is a tool developed by the CAIR (DRDO) for the use in Internet Monitoring System (IMS) of Department of Telecom. Authorized LEAs have access to IMS after due permission of competent authority as per legal provisions defined in section 69 of IT Act and Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009 read with the rules 22 and 23

(RAKESH KUMAR)
Under Secretary
Ministry of Home Affairs
Govt. of India, New Delhi

of the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009.

23. In view of the above, it is submitted that the extant safeguards are adequate and in place. Comprehensive guidelines, safeguards and SOP have been issued to provide safeguards; and the need to follow it has been reiterated to law enforcement/security agencies from time to time.

24. That the answering respondent craves leave of this Hon'ble to file a comprehensive Counter Affidavit, if necessary, as and when is directed to be filed by this Hon'ble Court.

PRAYER

In view of the submissions made hereinabove, it is respectfully prayed that this Hon'ble Court may kindly be pleased to dismiss the present writ petition being devoid of merit and no legal basis; and/or pass any such orders/directions that this Hon'ble Court may deem fit in the light of the above mentioned facts and circumstances of the case.

It is prayed accordingly.

DEPONENT

(राकेश कुमार)
(RAKESH KUMAR)
अवर सचिव
Under Secretary
गृह मंत्रालय
Ministry of Home
भारत सरकार, नई
Govt. of India, Ne

(15)

VERIFICATION: -

Verified at New Delhi on this the 5 JAN 2021 day of January, 2021 that the contents of the above affidavit are true and correct to my knowledge. No part of it is false and nothing material has been concealed there from.

DEPONENT

(राकेश कुमार)
(RAKESH KUMAR)
अवर सचिव
Under Secretary
Ministry of Home Affairs
Govt. of India, New Delhi

The Seal of Oath Commissioner
Sl. No. 73/05
NEELAM SHARMA
Advocate
NCT of Delhi
New Delhi

CERTIFIED THAT THE DEPONENT
Shri/Smt./Km.
S/o W/o D/o
R/o
identified
solemnly
on - 5 JAN 2021
that the
has been
are true
knowledge
Oath Commissioner New Delhi

- 5 JAN 2021

NOTIFICATION

New Delhi, the 27th October, 2009

G.S.R. 780 (E).— In exercise of the powers conferred by clause (y) of sub-section (2) of section 87, read with sub-section (2) of section 69 of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules, namely:

1. Short title and commencement.— (1) These rules may be called the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

(2) They shall come into force on the date of their publication in the Official Gazette.

2. Definitions.— In these rules, unless the context otherwise requires,–

(a) "Act" means the Information Technology Act, 2000 (21 of 2000);

(b) "communication" means dissemination, transmission, carriage of information or signal in some manner and include both a direct communication and an indirect communication";

(c) "communication link" means the use of satellite, microwave, radio, terrestrial line, wire, wireless or any other communication media to inter-connect computer resource;

(d) "competent authority" means –
(i) the Secretary in the Ministry of Home Affairs, in case of the Central Government; or
(ii) the Secretary in charge of the Home Department, in case of a State Government or Union territory, as the case may be;

(e) "computer resource" means computer resource as defined in clause (k) of sub-section (1) of section 2 of the Act;

(f) "decryption" means the process of conversion of information in non-intelligible form to an intelligible form via a mathematical formula, code, password or algorithm or a combination thereof;

(g) "decryption assistance" means any assistance to –
(i) allow access, to the extent possible, to encrypted information; or
(ii) facilitate conversion of encrypted information into an intelligible form;

(h) "decryption direction" means a direction issued under rule 3 in which a decryption key holder is directed to –
(i) disclose a decryption key; or
(ii) provide decryption assistance in respect of encrypted information

(i) "decryption key" means any key, mathematical formula, code, password, algorithm or any other data which is used to -
(i) allow access to encrypted information; or
(ii) facilitate the conversion of encrypted information into an intelligible form;

(j) "decryption key holder" means any person who deploys the decryption mechanism and who is in possession of a decryption key for purposes of subsequent decryption of encrypted information relating to direct or indirect communications;

(k) "information" means information as defined in clause (v) of sub-section (1) of section 2 of the Act;

(l) "intercept" with its grammatical variations and cognate expressions, means the aural or other acquisition of the contents of any information through the use of any means, including an interception device, so as to make some or all of the contents of a information available to a person other than the sender or recipient or intended recipient of that communication, and includes—
(a) monitoring of any such information by means of a monitoring device;
(b) viewing, examination or inspection of the contents of any direct or indirect information; and
(c) diversion of any direct or indirect information from its intended destination to any other destination;

(m) "interception device" means any electronic, mechanical, electro-mechanical, electro-magnetic, optical or other instrument, device, equipment or apparatus which is used or can be used, whether by itself or in combination with any other instrument, device, equipment or apparatus, to intercept any information; and any reference to an "interception device" includes, where applicable, a reference to a "monitoring device";

(n) "intermediary" means an intermediary as defined in clause (w) of sub-section (1) of section 2 of the Act;

(o) "monitor" with its grammatical variations and cognate expressions, includes to view or to inspect or listen to or record information by means of a monitoring device;

(राकेश कुमार)
(RAKESH KUMAR)
अवर सचिव
Under Secretary
गृह मंत्रालय
Ministry of Home Affairs
भारत सरकार, नई दिल्ली
Govt. of India, New Delhi

(o) "monitoring device" means any electronic, mechanical, electro-mechanical, electro-magnetic, optical or other instrument, device, equipment or apparatus which is used or can be used, whether by itself in combination with any other instrument, device, equipment or apparatus, to view or to inspect or to listen to or record any information;

(q) "Review Committee" means the Review Committee constituted under rule 419A of Indian Telegraph Rules, 1951.

3. Directions for interception or monitoring or decryption of any information.— No person shall carry out the interception or monitoring or decryption of any information generated, transmitted, received or stored in any computer resource under sub-section (2) of section 69 of the Act, except by an order issued by the competent authority:

Provided that in an unavoidable circumstances, such order may be issued by an officer, not below the rank of the Joint Secretary to the Government of India, who has been duly authorised by the competent authority:

Provided further that in a case of emergency–

(i) in remote areas, where obtaining of prior directions for interception or monitoring or decryption of information is not feasible; or

(ii) for operational reasons, where obtaining of prior directions for interception or monitoring or decryption of any information generated, transmitted, received or stored in any computer resource is not feasible,

the interception or monitoring or decryption of any information generated, transmitted, received or stored in any computer resource may be carried out with the prior approval of the Head or the second senior most officer of the security and law enforcement agency (hereinafter referred to as the said security agency) at the Central level and the officer authorised in this behalf, not below the rank of the Inspector General of Police or an officer of equivalent rank, at the State or Union territory level:

Provided also that the officer, who approved such interception or monitoring or decryption of information in case of emergency, shall inform in writing to the competent authority about the emergency and of such interception or monitoring or decryption within three working days and obtain the approval of the competent authority thereon within a period of seven working days and if the approval of competent authority is not obtained within the said period of seven working days, such interception or monitoring or decryption shall cease and the information shall not be intercepted or monitored or decrypted thereafter without the prior approval of the competent authority.

4. Authorisation of agency of Government.— The competent authority may authorise an agency of the Government to intercept, monitor or decrypt information generated, transmitted, received or stored in any computer resource for the purpose specified in sub-section (1) of section 69 of the Act.

5. Issue of decryption direction by competent authority.— The competent authority may, under rule 3 give any decryption direction to the decryption key holder for decryption of any information involving a computer resource or part thereof.

6. Interception or monitoring or decryption of information by a State beyond its jurisdiction.— Notwithstanding anything contained in rule 3, if a State Government or Union territory Administration requires any interception or monitoring or decryption of information beyond its territorial jurisdiction, the Secretary in-charge of the Home Department in that State or Union territory, as the case may be, shall make a request to the Secretary to the Ministry of Home Affairs, Government of India for issuing direction to the appropriate authority for such interception or monitoring or decryption of information.

7. Contents of direction.— Any direction issued by the competent authority under rule 3 shall contain reasons for such direction and a copy of such direction shall be forwarded to the Review Committee within a period of seven working days.

8. Competent authority to consider alternative means in acquiring information.— The competent authority shall, before issuing any direction under rule 3, consider possibility of acquiring the necessary information by other means and the direction under rule 3 shall be issued only when it is not possible to acquire the information by any other reasonable means.

(RAKESH KUMAR)
DIRECTOR
MINISTRY OF HOME AFFAIRS
GOVT. OF INDIA, NEW DELHI

9. Direction of interception or monitoring or decryption of any specific information.— The direction of interception or monitoring or decryption of any information generated, transmitted, received or stored in any computer resource shall be of any information as is sent to or from any person or class of persons or relating to any particular subject whether such information or class of information are received with one or more computer resources, or being a computer resource likely to be used for the generation, transmission, receiving, storing of information from or to one particular person or one or many set of premises, as may be specified or described in the direction.

10. Direction to specify the name and designation of the officer to whom information to be disclosed.— Every directions under rule 3 shall specify the name and designation of the officer of the authorised agency to whom the intercepted or monitored or decrypted or stored information shall be disclosed and also specify that the use of intercepted or monitored or decrypted information shall be subject to the provisions of sub-section (1) of section 69 of the said Act.

11. Period within which direction shall remain in force.— The direction for interception or monitoring or decryption shall remain in force, unless revoked earlier, for a period not exceeding sixty days from the date of its issue and may be renewed from time to time for such period not exceeding the total period of one hundred and eighty days.

12. Authorised agency to designate nodal officer.— The agency authorised by the competent authority under rule 4 shall designate one or more nodal officer, not below the rank of Superintendent of Police or Additional Superintendent of Police or the officer of the equivalent rank, to authenticate and send the requisition conveying direction issued under rule 3 for interception or monitoring or decryption to the designated officers of the concerned intermediaries or person in-charge of computer resource:

Provided that an officer, not below the rank of Inspector of Police or officer of equivalent rank, shall deliver the requisition to the designated officer of the intermediary.

13. Intermediary to provide facilities, etc.— (1) The officer issuing the requisition conveying direction issued under rule 3 for interception or monitoring or decryption of information shall also make a request in writing to the designated officers of intermediary or person in-charge of computer resources, to provide all facilities, co-operation and assistance for interception or monitoring or decryption mentioned in the directions.

(2) On the receipt of request under sub-rule (1), the designated officers of intermediary or person in-charge of computer resources, shall provide all facilities, co-operation and assistance for interception or monitoring or decryption of information mentioned in the direction.

(3) Any direction of decryption of information issued under rule 3 to intermediary shall be limited to the extent the information is encrypted by the intermediary or the intermediary has control over the decryption key.

14. Intermediary to designate officers to receive and handle requisition.— Every intermediary or person in-charge of computer resource shall designate an officer to receive requisition, and another officer to handle such requisition, from the nodal officer for interception or monitoring or decryption of information generated, transmitted, received or stored in any computer resource.

15. Acknowledgement of instruction.— The designated officer of the intermediary or person in-charge of computer resources shall acknowledge the instructions received by him through letters or fax or e-mail signed with electronic signature to the nodal officer of the concerned agency within two hours on receipt of such intimation or direction for interception or monitoring or decryption of information.

(राकेश कुमार)
(RAKESH KUMAR)
अवर सचिव
Under Secretary
गृह मंत्रालय
Ministry of Home Affairs
भारत सरकार, नई दिल्ली
Govt. of India, New Delhi

16. Maintenance of records by designated officer.— The designated officer of intermediary or person in-charge of computer resource authorised to intercept or monitor or decrypt any information shall maintain proper records mentioning therein, the intercepted or monitored or decrypted information, the particulars of persons, computer resource, e-mail account, website address, etc. whose information has been intercepted or monitored or decrypted, the name and other particulars of the officer or the authority to whom the intercepted or monitored or decrypted information has been disclosed, the number of copies, including corresponding electronic records of the intercepted or monitored or decrypted information made and the mode or the method by which such copies, including corresponding electronic record are made, the date of destruction of the copies, including corresponding electronic record and the duration within which the directions remain in force.

17. Decryption key holder to disclose decryption key or provide decryption assistance.— If a decryption direction or a copy thereof is handed to the decryption key holder to whom the decryption direction is addressed by the nodal officer referred to in rule 12, the decryption key holder shall within the period mentioned in the decryption direction —

(a) disclose the decryption key; or

(b) provide the decryption assistance,

specified in the decryption direction to the concerned authorised person.

18. Submission of list of interception or monitoring or decryption of information.— (1) The designated officers of the intermediary or person in-charge of computer resources shall forward in every fifteen days a list of interception or monitoring or decryption authorisations received by them during the preceding fortnight to the nodal officers of the agencies authorised under rule 4 for confirmation of the authenticity of such authorisations.

(2) The list referred to in sub-rule (1) shall include details, such as the reference and date of orders of the concerned competent authority including any order issued under emergency cases, date and time of receipt of such order and the date and time of implementation of such order.

19. Intermediary to ensure effective check in handling matter of interception or monitoring or decryption of information.— The intermediary or the person in-charge of the computer resource so directed under rule 3, shall provide technical assistance and the equipment including hardware, software, firmware, storage, interface and access to the equipment wherever requested by the agency authorised under rule 4 for performing interception or monitoring or decryption including for the purposes of-

(i) the installation of equipment of the agency authorised under rule 4 for the purposes of interception or monitoring or decryption or accessing stored information in accordance with directions by the nodal officer; or

(ii) the maintenance, testing or use of such equipment; or

(iii) the removal of such equipment; or

(iv) the performance of any action required for accessing of stored information under the direction issued by the competent authority under rule 3.

20. Intermediary to ensure effective check in handling matter of interception or monitoring or decryption of information.— The intermediary or person in-charge of computer resources shall put in place adequate and effective internal checks to ensure the unauthorised interception of information does not take place and extreme secrecy is maintained and utmost care and precaution shall be taken in the matter of interception or monitoring or decryption of information as it affects privacy of citizens and also that it is handled only by the designated officers of the intermediary and not other person of the intermediary or person in-charge of computer resources shall have access to such intercepted or monitored or decrypted information.

21. Responsibility of intermediary.— The intermediary or person in-charge of computer resources shall be responsible for any action of their employees also and in case of violation pertaining to maintenance of secrecy and confidentiality of information or any unauthorised interception or monitoring or decryption of information, the intermediary or person in-charge of computer resources shall be liable for any action under the relevant provisions of the laws for the time being in force..

22. Review of directions of competent authority.— The Review Committee shall meet at least once in two months and record its findings whether the directions issued under rule 3 are in accordance with the provisions of sub-section (2) of section 69 of the Act and where the Review Committee is of the opinion that the directions are not in accordance with the provisions referred to above, it may set aside the directions and issue order for destruction of the copies, including corresponding electronic record of the intercepted or monitored or decrypted information.

23. Destruction of records of interception or monitoring or decryption of information.— (1) Every record, including electronic records pertaining to such directions for interception or monitoring or decryption of information and of intercepted or monitored or decrypted information shall be destroyed by the security agency in every six months except in a case where such information is required, or likely to be required for functional requirements.

(राकेश कुमार)
(RAKESH KUMAR)
अवर सचिव
Under Secretary
गृह मंत्रालय
Ministry of Home Affairs
भारत सरकार, नई दिल्ली
Govt. of India, New Delhi

(2) Save as otherwise required for the purpose of any ongoing investigation, criminal complaint or legal proceedings, the intermediary or person in-charge of computer resources shall destroy records pertaining to directions for interception of information within a period of two months of discontinuance of the interception or monitoring or decryption of such information and in doing so they shall maintain extreme secrecy.

24. Prohibition of interception or monitoring or decryption of information without authorisation.— (1) Any person who intentionally or knowingly, without authorisation under rule 3 or rule 4, intercepts or attempts to intercept, or authorises or assists any other person to intercept or attempts to intercept any information in the course of its occurrence or transmission at any place within India, shall be proceeded against and punished accordingly under the relevant provisions of the laws for the time being in force.

(2) Any interception, monitoring or decryption of information in computer resource by the employee of an intermediary or person in-charge of computer resource or a person duly authorised by the intermediary, may be undertaken in course of his duty relating to the services provided by that intermediary, if such activities are reasonably necessary for the discharge his duties as per the prevailing industry practices, in connection with the following matters, namely—

(i) installation of computer resource or any equipment to be used with computer resource; or

(ii) operation or maintenance of computer resource; or

(iii) installation of any communication link or software either at the end of the intermediary or subscriber, or installation of user account on the computer resource of intermediary and testing of the same for its functionality;

(iv) accessing stored information from computer resource relating to the installation, connection or maintenance of equipment, computer resource or a communication link or code; or

(v) accessing stored information from computer resource for the purpose of—

(a) implementing information security practices in the computer resource;

(b) determining any security breaches, computer contaminant or computer virus;

(c) undertaking forensic of the concerned computer resource as a part of investigation or internal audit; or

(vi) accessing or analysing information from a computer resource for the purpose of tracing a computer resource or any person who has contravened, or is suspected of having contravened or being likely to contravene any provision of the Act that is likely to have an adverse impact on the services provided by the intermediary.

(3) The intermediary or the person in-charge of computer resource and its employees shall maintain strict secrecy and confidentiality of information while performing the actions specified under sub-rule (2).

25. Prohibition of disclosure of intercepted or monitored or decrypted information.— (1) The contents of intercepted or monitored or stored or decrypted information shall not be used or disclosed by intermediary or any of its employees or person in-charge of computer resource to any person other than the intended recipient of the said information under rule 10.

(2) The contents of intercepted or monitored or decrypted information shall not be used or disclosed by the agency authorised under rule 4 for any other purpose, except for investigation or sharing with other security agency for the purpose of investigation or in judicial proceedings before the competent court in India.

(3) Save as otherwise provided in sub-rule (2), the contents of intercepted or monitored or decrypted information shall not be disclosed or reported in public by any means, without the prior order of the competent court in India.

(4) Save as otherwise provided in sub-rule (2), strict confidentiality shall be maintained in respect of direction for interception, monitoring or decryption issued by concerned competent authority or the nodal officers.

(राकेश कुमार)
(RAKESH KUMAR)
अवर सचिव
Under Secretary
गृह मंत्रालय
Ministry of Home Affairs
भारत सरकार, नई दिल्ली
Govt. of India, New Delhi

(5) Any intermediary or its employees or person in-charge of computer resource who contravenes provisions of these rules shall be proceeded against and punished accordingly under the relevant provisions of the Act for the time being in force.

(6) Whenever asked for by the concerned security agency of the Centre, the security agencies of the State and the Union territory level shall promptly share any information which they may have obtained following directions for interception or monitoring or decryption of any information generated, transmitted, received or stored in any computer resource under rule 3, with the security agency of the Centre.

[No. 9(16)/2004-EC]
N. RAVI SHANKER, Jt. Secy.

(राकेश कुमार)
(RAKESH KUMAR)
अवर सचिव
Under Secretary
गृह मंत्रालय
Ministry of Home Affairs
भारत सरकार, नई दिल्ली
Govt. of India, New Delhi

18. सा.का.नि. 674(अ), दिनांक 27.7.1987
19. सा.का.नि. 719(अ), दिनांक 18.8.1987
20. सा.का.नि. 837(अ), दिनांक 5.10.1987
21. सा.का.नि. 989(अ), दिनांक 17.12.1987
22. सा.का.नि. 337(अ), दिनांक 11.3.1988
23. सा.का.नि. 361(अ), दिनांक 11.3.1988
24. सा.का.नि. 626(अ), दिनांक 17.5.1988
25. सा.का.नि. 660(अ), दिनांक 31.5.1988
26. सा.का.नि. 693(अ), दिनांक 10.6.1988
27. सा.का.नि. 734(अ), दिनांक 24.6.1988
28. सा.का.नि. 606(अ), दिनांक 14.7.1988
29. सा.का.नि. 812(अ), दिनांक 26.7.1988
30. सा.का.नि. 888(अ), दिनांक 1.9.1988
31. सा.का.नि. 907(अ), दिनांक 7.9.1988
32. सा.का.नि. 916(अ), दिनांक 9.9.1988
33. सा.का.नि. 1054(अ), दिनांक 2.11.1988
34. सा.का.नि. 179, दिनांक 18.3.1989
35. सा.का.नि. 358(अ), दिनांक 15.3.1989
36. सा.का.नि. 622(अ), दिनांक 15.6.1989
37. सा.का.नि. 865(अ), दिनांक 29.9.1989
38. सा.का.नि. 413(अ), दिनांक 29.3.1990
39. सा.का.नि. 574(अ), दिनांक 15.6.1990
40. सा.का.नि. 933(अ), दिनांक 3.12.1990
41. सा.का.नि. 985(अ), दिनांक 20.12.1990
42. सा.का.नि. 74(अ), दिनांक 18.1.1991
43. सा.का.नि. 237(अ), दिनांक 25.4.1991
44. सा.का.नि. 251(अ), दिनांक 2.5.1991
45. सा.का.नि. 543(अ), दिनांक 21.5.1992
46. सा.का.नि. 560(अ), दिनांक 26.5.1992
47. सा.का.नि. 587(अ), दिनांक 10.6.1992
48. सा.का.नि. 730(अ), दिनांक 19.8.1992
49. सा.का.नि. 830(अ), दिनांक 28.10.1992
50. सा.का.नि. 62(अ), दिनांक 11.2.1993
51. सा.का.नि. 80, दिनांक 6.2.1993
52. सा.का.नि. 384(अ), दिनांक 27.4.1993
53. सा.का.नि. 387(अ), दिनांक 28.4.1993
54. सा.का.नि. 220(अ), दिनांक 26.3.2004
55. सा.का.नि. 713(अ), दिनांक 17.11.2006
56. सा.का.नि. 193(अ), दिनांक 1.3.2007
57. सा.का.नि. 547(अ), दिनांक 18.7.2008
58. सा.का.नि. 49(अ), दिनांक 27.1.2010
59. सा.का.नि. 279(अ), दिनांक 31.3.2010
60. सा.का.नि. 256(अ), दिनांक 27.3.2012
61. सा.का.नि. 412(अ), दिनांक 29.5.2012
62. सा.का.नि. 368(अ), दिनांक 7.6.2012
63. सा.का.नि. 506(अ), दिनांक 24.7.2012

(राकेश कुमार)
(RAKESH KUMAR)
अवर सचिव
Under Secretary
भारत सरकार
Ministry of Communications & IT
संचार एवं सूचना प्रौद्योगिकी मंत्रालय
Govt. of India, New Delhi

MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY

(Department of Telecommunications)

New Delhi, the 28th January, 2014

G.S.R. 18.—In exercise of the powers conferred by section 7 of the Indian Telegraph Act, 1885 (13 of 1885), the Central Government hereby makes the following rules further to amend the Indian Telegraph Rules, 1951, namely:—

1. (1) These rules may be called the Indian Telegraph (1st Amendment of 2014) Rules, 2014.

(2) They shall come into force on the date of their publication in the Official Gazette.

2. In the Indian Telegraph Rules, 1951, for rule 419A, the following rule shall be substituted, namely :-

"**419A.** (1) Directions for interception of any message or class of messages under sub-section (2) of section 5 of the Indian Telegraph Act, 1885 (hereinafter referred to as the said Act) shall not be issued except by an order made by the Secretary to the Government of India in the Ministry of Home Affairs in the case of Government of India and by the Secretary to the State Government in-charge of the Home Department in the case of a State Government and in unavoidable circumstances, such order may be made by an officer, not below the rank of a Joint Secretary to the Government of India, who has been duly authorised by the Union Home Secretary or the State Home Secretary, as the case may be:

Provided that in emergent cases —

(i) in remote areas, where obtaining of prior directions for interception of messages or class of messages is not feasible; or

(ii) for operational reasons, where obtaining of prior directions for interception of messages or class of messages is not feasible,

the required interception of any message or class of messages shall be carried out with the prior approval of the Head or the second senior most officer of the authorised Security and Law Enforcement Agency at the Central Level and the officers authorised in this behalf, not below the rank of Inspector General of Police, at the

State level but the concerned competent authority shall be informed of such interceptions by the approving authority within three working days and that such interceptions shall be got confirmed by the concerned competent authority within a period of seven working days and if the confirmation from the competent authority is not received within the stipulated seven days, such interception shall cease and the same message or class of messages shall not be intercepted thereafter without the prior approval of the Union Home Secretary or the State Home Secretary, as the case may be.

(2) Any order issued by the competent authority under sub-rule (1) shall contain reasons for such direction and a copy of such order shall be forwarded to the concerned Review Committee within a period of seven working days.

(3) While issuing directions under sub-rule (1), the officer shall consider possibility of acquiring the necessary information by other means and the directions under sub rule (1) shall be issued only when it is not possible to acquire the information by any other reasonable means.

(4) The interception directed shall be the interception of any message or class of messages as are sent to or from any person or class of persons or relating to any particular subject whether such message or class of messages are received with one or more addresses, specified in the order, being an address or addresses likely to be used for the transmission of communications from or to one particular person specified or described in the order or one particular set of premises specified or described in the order.

(5) The directions shall specify the name and designation of the officer or the authority to whom the intercepted message or class of messages is to be disclosed and also specify that the use of intercepted message or class of messages shall be subject to the provisions of sub-section (2) of section 5 of the said Act.

(6) The directions for interception shall remain in force, unless revoked earlier, for a period not exceeding sixty days from the date of issue and may be renewed but the same shall not remain in force beyond a total period of one hundred and eighty days.

(7) The directions for interception issued under sub-rule (1) shall be conveyed to designated officers of the telegraph authority or to the designated officers of the service provider(s) who have been granted licences under section 4 of the said Act, in writing or by secure electronic communication by an officer not below the rank of Superintendent of Police or the officer of the equivalent rank and mode of secure electronic communication and its implementation shall be as determined by the telegraph authority.

(8) The officer authorised to intercept any message or class of messages shall maintain proper records mentioning therein, the intercepted message or class of messages, the particulars of persons whose message has been intercepted, the name and other particulars of the officer or the authority to whom the intercepted message or class of messages has been disclosed, the number of copies of the intercepted message or class of messages made and the mode or the method by which such copies are made, the date of destruction of the copies and the duration within which the directions remain in force.

(9) All the requisitioning Security and Law Enforcement Agencies shall designate one or more nodal officers not below the rank of Superintendent of Police or the officer of the equivalent rank to authenticate and send the requisitions for interception to the designated officers of the telegraph authority or the concerned service providers, as the case may be and the delivery of written requisition for interception shall be done by an officer not below the rank of Sub-Inspector of Police.

(10) The telegraph authority shall designate officer(s) in every licensed service area / State / Union territory as the nodal officers to receive and handle such requisitions for interception and the service providers shall designate two senior officer(s) of the company in every licensed service area / State / Union territory as the nodal officers to receive and handle such requisitions for interception.

(11) The designated nodal officer(s) of the telegraph authority or the service providers shall issue acknowledgment to the requisitioning Security and Law Enforcement Agency within two hours on receipt of intimations for interception.

(12) The system of designated nodal officers for communicating and receiving the requisitions for interceptions shall also be followed in emergent cases / unavoidable cases where prior approval of the competent authority has not been obtained.

(13) The designated nodal officer(s) of the telegraph authority or the service providers shall forward every fifteen days a list of interception authorisations received by them during the preceding fortnight to the nodal officers of the Security and Law Enforcement Agencies for confirmation of the authenticity of such authorisations and the list shall include details such as the reference and date of orders of the Union Home Secretary or State Home Secretary or orders issued by officer other than competent authority, in terms of sub-rule (1) in emergent cases which were not subsequently confirmed by the competent authority, date and time of receipt of such orders and the date and time of implementation of such orders.

358 GI/14-2

(राकेश कुमार)
(RAKESH KUMAR)
अवर सचिव
Under Secretary
गृह मंत्रालय
Ministry of Home Affairs
भारत सरकार, नई दिल्ली
Govt. of India, New Delhi

(14) The service providers shall put in place adequate and effective internal checks to ensure that unauthorised interception of messages does not take place and extreme secrecy is maintained and utmost care and precaution is taken in the matter of interception of messages as it affects privacy of citizens and also that this matter is handled only by the designated nodal officers of the company.

(15) The service providers shall be responsible for actions of their employees also and in case of established violation of licence conditions pertaining to maintenance of secrecy and confidentiality of information and unauthorised interception of communication, action shall be taken against the service providers as per provisions of the said Act, and this shall include not only fine but also suspension or revocation of their licences.

(16) The Central Government and the State Government, as the case may be, shall constitute a Review Committee.

(i) The Review Committee to be constituted by the Central Government shall consist of the following, namely:-

(a)	Cabinet Secretary	—Chairman;
(b)	Secretary to the Government of India Incharge, Legal Affairs	Member;
(c)	Secretary to the Government, Department of Telecommunications	Member.

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

(a)	Chief Secretary	Chairman;
(b)	Secretary Law/Legal Remembrancer Incharge, Legal Affairs	Member;
(c)	Secretary to the State Government (other than the Home Secretary)	Member.

(17) The Review Committee shall meet at least once in two months and record its findings whether the directions issued under sub-rule (1) are in accordance with the provisions of sub-section (2) of section 5 of the said Act and when the Review Committee is of the opinion that the directions are not in accordance with the provisions referred to above, it may set aside the directions and orders for destruction of the copies of the intercepted message or class of messages.

(18) Records pertaining to such directions for interception and of intercepted messages shall be destroyed by the relevant competent authority and the authorised Security and Law Enforcement Agencies every six months unless these are, or likely to be, required for functional requirements.

(19) The service providers and telegraph authority shall destroy records pertaining to directions for interception of messages within two months of discontinuance of the interception of such messages and in doing so they shall maintain extreme secrecy".

[F. No. 4-19/2009-PHP]

S. S. SINGH, Dy. Director General (PG)
Cum-Ex-Officio Jt. Secy.

NOTE: The principal rules were published in the Post and Telegraph Manual Volume I, Legislative Enactments, Part II, Edition and subsequently amended vide notification numbers—

1. GS.R. 190, dated 18-2-1984
2. GS.R. 386, dated 22-5-1984
3. GS.R. 387(E), dated 22-5-1984
4. GS.R. 679, dated 30-6-1984
5. GS.R. 428, dated 27-4-1985
6. GS.R. 729, dated 3-8-1985
7. GS.R. 982, dated 19-10-1986
8. GS.R. 553(E), dated 27-03-1986
9. GS.R. 314, dated 26-4-1986
10. GS.R. 566, dated 26-7-1986
11. GS.R. 953(E), dated 23-7-1986
12. GS.R. 1121(E), dated 1-10-1986
13. GS.R. 1167(E), dated 28-10-1986
14. GS.R. 1237(E), dated 28-11-1986
15. GS.R. 49, dated 17-1-1987
16. GS.R. 112(E), dated 25-2-1987
17. GS.R. 377(E), dated 9-4-1987
18. GS.R. 674(E), dated 27-7-1987
19. GS.R. 719(E), dated 18-8-1987
20. GS.R. 837(E), dated 5-10-1987
21. GS.R. 989(E), dated 17-12-1987
22. GS.R. 337(E), dated 11-3-1988
23. GS.R. 361(E), dated 21-3-1988
24. GS.R. 626(E), dated 17-5-1988
25. GS.R. 660(E), dated 31-5-1988
26. GS.R. 693(E), dated 10-6-1988
27. GS.R. 734(E), dated 24-6-1988
28. GS.R. 606, dated 14-7-1988
29. GS.R. 812(E), dated 26-7-1988
30. GS.R. 888(E), dated 1-9-1988
31. GS.R. 907(E), dated 7-9-1988

(राकेश कुमार)
(RAKESH KUMAR)
अवर सचिव
Under Secretary
गृह मंत्रालय
Ministry of Home Affairs
भारत सरकार, नई दिल्ली
Govt. of India, New Delhi

Gmail pawan singh <ps431999@gmail.com>

Fwd: Filing of Short Affidavit in W.P.(C) NO. 8998/2020 titled as “Centre for PIL & Anr. Vs. Union of India & Ors.

2 messages

Mukesh kumar <mukesh.digpaulassociates@gmail.com> Tue, Jan 5, 2021 at 5:46 PM
To: ps431999@gmail.com

---------- Forwarded message ---------
From: **Yogesh Kumar** <yogeshwar.digpaulassociates@gmail.com>
Date: Tue, 5 Jan, 2021, 5:46 pm
Subject: Filing of Short Affidavit in W.P.(C) NO. 8998/2020 titled as “Centre for PIL & Anr. Vs. Union of India & Ors.
To: <hari.shubham@gmail.com>, <prashantbhush@gmail.com>, <mail@mcalaw.in>
Cc: digpaulassociates <digpaulassociates@yahoo.co.in>, mukesh.digpaulassociates <mukesh.digpaulassociates@gmail.com>, Kamal Digpaul <kamaldigpaul@gmail.com>

Dated : 05.01.2021

To,

Mr. Prashant Bhushan,
Counsel for the petitioner
301, New Lawyers Chamber,
Supreme Court of India,
New Delhi-110001.
Mobile No: +9 1-981 1 164068
E-mail: hari.shubham@gmail.com
prashantbhush@gmail.com
mail@mcalaw.in

Sub- Filing of Short Affidavit in W.P.(C) NO. 8998/2020 titled as “Centre for PIL & Anr. Vs. Union of India & Ors.

Dear sir,

This is to inform you that the subject matter is listed for hearing on 07.01.2021.

We are hereby filing a Short Affidavit in the subject matter on behalf of the respondent Nos. 2, 3 & 4/UOI and a copy thereof is being served upon you towards advance service.

Please acknowledge the same.

Thanking You.

Yours Sincerely,

Ajay Digpaul, Advocate
Central Govt. Standing Counsel
Chamber No. 138-139, Patiala House Court,
New Delhi-110001.
Phone No.: 011-23387119, 23382949
Mobile: 9811157265, 9818276507

Short Affidavit by R-2 to 4--Centre for PIL Vs. UOI & Ors.-WPC No. 8998_2020.pdf
1154K

Mukesh kumar <mukesh.digpaulassociates@gmail.com> Wed, Feb 3, 2021 at 5:40 PM
To: ps431999@gmail.com

---------- Forwarded message ---------
From: **Yogesh Kumar** <yogeshwar.digpaulassociates@gmail.com>
Date: Tue, 2 Feb, 2021, 4:36 pm
Subject: Fwd: Filing of Short Affidavit in W.P.(C) NO. 8998/2020 titled as “Centre for PIL & Anr. Vs. Union of India & Ors.
To: <hari.shubham@gmail.com>, <prashantbhush@gmail.com>, <mail@mcalaw.in>

Cc: digpaulassociates <digpaulassociates@yahoo.co.in>, Kamal Digpaul <kamaldigpaul@gmail.com>, mukesh.digpaulassociates <mukesh.digpaulassociates@gmail.com>

Dated : 02.02.2021

[Quoted text hidden]

Short Affidavit by R-2 to 4--Centre for PIL Vs. UOI & Ors.-WPC No. 8998_2020.pdf
1154K