IN THE SUPREME COURT OF INDIA

CIVIL ORIGINAL JURISDICTION

WRIT PETITION (CIVIL) NO. OF 2019

IN THE MATTER OF:-

Internet Freedom Foundation & Another … PETITIONERS

VERSUS

Union of India & Others … RESPONDENTS

ALONG WITH

I.A. No. of 2019 An Application seeking *ex-parte* Interim Stay / Directions

VOLUME – I

PAGE NOS. A - 231

SYNOPSIS, LIST OF DATES, WRIT PETITION & ANNEXURE P-1 TO P-13

PAPERBOOK

(KINDLY SEE INSIDE FOR INDEX)

PRATEEK CHADDHA

ADVOCATE FOR THE PETITIONERS

SYNOPSIS

The present Writ Petition under Article 32 of the Constitution of India, filed in public interest, seeks to challenge the constitutional validity of:-

i. Section 69 of the Information Technology Act, 2000 ["**IT Act**"].

ii. The Information Technology (Procedure for Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 ["**2009 IT Rules**"] enacted pursuant to Section 69(2) read with Section 87(2)(y) of the IT Act.

iii. The Notification dated 20.12.2018 (bearing No. 14/07/2011-T) ["**Impugned Notification**"], wherein ten (10) Security and Intelligence Agencies ["**Authorised Agencies**"] of the Central Government have been authorised to intercept, monitor, and decrypt [collectively described as "**Electronic Surveillance**"] any information generated, transmitted, received, or stored in any computer resource.

The Impugned Notification, the first of its kind issued under Section 69(2) of the IT Act read with Rule 4 of the 2009 IT Rules, has essentially activated the unconstitutional surveillance mechanism erected by the Act and Rules, necessitating urgent intervention by this Hon'ble Court, especially since the institutional structure created provides for no judicial oversight which, as shall be elaborated hereunder, would be a minimum requirement for the provisions in question to pass muster from a constitutional standpoint. It is the Petitioners' case that the Impugned Provisions, i.e. Section 69 of the IT Act and the 2009 IT Rules, as also the Impugned Notification, are violative of Articles 14, 19, 20 and 21 of the Constitution of India and, specifically, impact the right to privacy and fail the test of proportionality, the substantive contents of which have been articulated

in **K. S. Puttaswamy v. Union of India** (2017) 10 SCC 1 ["**Puttaswamy (*Privacy*)**"] and **K. S. Puttaswamy v. Union of India** (2018) 12 SCALE 1 ["**Puttaswamy (*Aadhaar*)**"].

Petitioner No. 1 herein, i.e. the Internet Freedom Foundation ["**IFF**"], is a registered charitable Trust, setup *inter alia* to protect, promote and defend human rights of citizens using information communication technologies, and it has proactively intervened and assisted courts in India on cases affecting the rights of citizens for an open, equitable and secure access to the Internet. The Petitioner-Trust is deeply concerned by the pervasive, sweeping, and clandestine activities of the State to intercept, monitor, and decrypt communications and other data generated, stored, shared, or transmitted through digital platforms.

The Petition submits that the relaxation of the rules of *locus standi* and the jurisprudential evolution of PILs is oriented towards this Hon'ble Court functioning as the last bulwark of liberty in cases precisely like the present one, where there is little scope for the subject of surveillance to approach a Court in specific instances, since the system itself is covert.

Therefore, with little or no possibility of individuals detecting and complaining of legal injury, it is imperative for this Hon'ble Court to test the constitutionality of the surveillance system erected by the impugned provisions along with the impugned notification, especially since its very existence, in the absence of any independent oversight, impacts the fundamental rights of citizens.

i. First and foremost, the very act of surveillance – taken on its own – infringes fundamental rights under Articles 19(1)(a) and 21. While the "harm" that surveillance causes cannot be quantified in a physical or tangible form, this Hon'ble Court has never insisted

upon a showing of physical injury as a threshold requirement to demonstrate the violation of a fundamental right. The Petitioners respectfully submit that the very existence of a surveillance system impacts the right to privacy and chills the exercise of liberties under Articles 19 and 21, and prevents people from thinking about, reading and exchanging unorthodox, controversial or provocative ideas. Regardless of whether or not a citizen knows that her email is being read by the government, the perceived danger, founded on reasonable suspicion that this may happen, itself impacts the citizen's ability to express, receive and discuss such ideas. This was explained by Justice Subba Rao in his dissenting opinion in **Kharak Singh v Union of India,** [1964] 1 SCR 332, and has, most recently, been upheld by this Hon'ble Court in **Puttaswamy** (*Privacy*).

ii. Second, in the absence of parliamentary or judicial oversight, such electronic surveillance gives the executive government the power to influence the subject of surveillance as well as all classes of persons. This is particularly dangerous since the provision is agnostic with respect to the subject of surveillance, and surveillance takes place without any checks outside the executive wing of government. The very existence of such disproportionate power vesting with one wing of government would violate not only Part III of the Constitution, which impacts the vertical relationship between the citizen and the State; but would also impact the horizontal separation of power between the executive, legislature and judiciary.

The fact that surveillance, particularly a structure such as the one erected by the Impugned Provisions and the Impugned Notification, seriously impacts the right to privacy is a proposition that is no longer *res integra*. This Court has taken this view in **People's Union for Civil Liberties v. Union of India** (1997) 1 SCC 301 (the "**Wiretapping**

Judgment"), and this view has subsequently been upheld in **Puttaswamy** (*Privacy*) and **Puttaswamy** (*Aadhaar*).

Given that violation of the fundamental right to privacy is apparent *ex facie*, the next question which would arise is whether the Impugned Provisions and Notification would survive scrutiny based on the proportionality standard. Apart from establishing that a law impacting privacy subserves a legitimate goal, and that such a measure is rationally connected to such goal, it must also be established (in order for such a government measure to survive scrutiny): -

i. That there are no alternative less invasive measures (i.e. the test of necessity)

ii. The measure must not have a disproportionate impact on the right holder (balancing stage), i.e. there is a proper relation between the importance of achieving the aim and importance of limiting the right.

Additionally, as established in **Puttaswamy** (*Privacy*), there must also be adequate procedural safeguards in place, for such a measure to pass muster.

This schema to analyze the violation of privacy rights was not a part of our jurisprudence when this Hon'ble Court took a lenient view of the absence of judicial oversight while dealing with Section 5(2) of the Telegraph Act in the **Wiretapping Judgment**. It is the Petitioners case that, in light of the law laid down in **Puttaswamy** (*Privacy*) and **Puttaswamy** (*Aadhaar*), the lack of any oversight, in itself, warrants a finding that the Impugned Provisions and the Impugned Notification are unconstitutional for the following reasons: -

i. Apart from disturbing the horizontal separation of powers, as mentioned hereinabove, the concentration of disproportionate

power in the hands of the executive under the Impugned Provisions and Impugned Notification would violate the requirement of having adequate procedural safeguards, as mandated in **Puttaswamy** (*Privacy*). Therefore, oversight by another branch of government would be the minimum requirement for surveillance provisions to pass muster.

ii. Specifically, based on the rulings in **Puttaswamy** (*Privacy*) and **Puttaswamy** (*Aadhaar*), judicial oversight would be the minimum requirement for this system to pass constitutional muster, as the judiciary alone is competent to decide whether specific instances of surveillance are proportionate, especially to decide whether less onerous alternatives are available and in balancing the importance of the government objective with the rights of the individual / individuals impacted. It is obvious that a Court, alone, is competent to decide the constitutionality of individual instances of surveillance and test it on the proportionality standard. Nothing in the Court rulings in **Puttaswamy** (*Privacy*) and **Puttaswamy** (*Aadhaar*) suggests that a finding on proportionality can be returned by an executive authority.

iii. However, the requirement of judicial oversight goes beyond the issue of institutional competence. It is also an minimum requirement in order to satisfy the requirement of "due process". By design, surveillance - which operates in secret - curtails the operation of Articles 32 and 226 of the Constitution, as a person who suspects that she is under surveillance, in many cases will have no way of proving it, and cannot therefore establish a breach in accordance with Articles 32 and 226, until that information is revealed. The effective exclusion of Articles 32 and 226 therefore entails that, for all practical purposes, the decision of the Executive on whether fundamental rights have been validly and reasonably infringed, is final. It is respectfully

submitted that this violates the requirements of fairness and due process under Article 21, as well as the broader requirements of natural justice. This denial of judicial scrutiny amounts to an effective denial of remedies under Article 21 of the Constitution. In the absence of a judicial determination that surveillance meets the proportionality standards under Article 21, the lack of ability to approach the courts effectively entails the denial of the right itself.

iv. Additionally, authorizing incursions into the private domain in the course of "investigation" is, traditionally, within the exclusive domain of the judiciary alone (akin to the judiciary's power to issue warrants for search and seizure of premises), and the fact that Section 69 of the IT Act can be deployed in the investigation of criminal offences without any judicial oversight buttresses the Petitioners case that the Impugned Provisions and the Impugned Notification run contrary to the horizontal separation of powers established under the Constitution of India.

In addition to absence of oversight, the Petitioners also contend that the substantive provisions of the Act and the Rules also fail the test of proportionality. Most of the grounds specified under Section 69(1) to carry out electronic surveillance are a verbatim reproduction of restrictions contained in Article 19(2). Consequently, the Executive has an unguided discretion to justify electronic surveillance. Notably, the provision also encompasses circumstances relating to "defence of India," although such an expression is neither defined under the IT Act nor recognised under Article 19(2). Egregiously, the provision enables the State to conduct perpetual, untargeted, and mass surveillance of her citizens, under a pretext for "investigation of *any* offence".

Further, while secrecy may be an inherent trait, and even the paramount objective for carrying out electronic surveillance, the IT Act

and 2009 Rules have, while excessively delegating to the Executive, failed to instil adequate safeguards to prevent abusive, excessive, and arbitrary exercise of its powers. In particular, the "necessary or expedient" standard adopted under sub-clause (1) of Section 69 to authorise electronic surveillance woefully falls short of "the test of proportionality" - a sine-qua-non to curtail fundamental rights under Articles 19(1)(a) and 21.

It may also be remembered that the **Wiretapping judgment** dealt with Section 5(2) of the Telegraph Act, which requires a public emergency or an issue of public safety for the provision to even be triggered. Despite the fact that surveillance under the IT Act is not only comparable, but is perhaps more invasive than telephone tapping, there is no explanation for why this higher threshold of public emergency/public safety is absent from Section 69 of the IT Act. This inexplicable difference in Section 5(2) of the Telegraph Act and Section 69 of the IT Act, in itself, is evidence that Section 69 of the IT Act is capricious and irrational. For this, and other reasons, the Petitioners contend that the Impugned Provisions and Impugned Notification suffer from the vice of manifest arbitrariness, apart from the fact that they are overbroad and unconstitutionally vague.

On these, and other grounds (as set out in the Writ Petition), the Petitioners herein have been constrained to approach this Hon'ble Court under Article 32 of the Constitution of India, in public interest.

LIST OF DATES

1972 By virtue of Telegraph (Amendment) Act, 1972, Section 5(2) of the Telegraph Act, 1885 was amended to authorise the Central and State Governments, or any officers on their behalf, to lawfully intercept or detain

messages transmitted by individuals through the 'telegraph'.

18.12.1996 This Hon'ble Court in **People's Union for Civil Liberties v. Union of India** (1997) 1 SCC 301 ("**Wiretapping Judgment**") issued a series of safeguards to the Executive in phone tapping, to protect the fundamental rights of citizens.

2007 Almost a decade later, the Central Government inserted Rule 419A to the Telegraph Rules, 1951 to codify the binding direction issued by this Hon'ble in the PUCL **Wiretapping judgment** (*supra*).

05.02.2009 By virtue of Information Technology (Amendment) Act, 2008, the Parliament amended Section 69 of the IT Act (impugned herein) to permit the Executive to "monitor" and "decrypt" electronic communications, in addition to interception. Moreover, the Amendment also introduced two additional grounds (viz., 'defence of India' and 'investigation of any offence') to cause electronic surveillance, which were not present in the Telegraph Act.

27.10.2009 The Information Technology (Procedure for Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 ["**2009 IT Rules**"] enacted pursuant to Section 69(2) read with Section 87(2)(y) of the Act was brought into force. The provisions contained therein are similar to safeguards contained in Rule 419A of the Telegraph Rules.

20.12.2010 According to a report published in India Today, it was found that more than 6,000 telephones were under watch in New Delhi alone. The list included bureaucrats, military officials, corporates, journalist and NGOs.

16.10.2012 The 'Report by the Group of Experts' constituted by the Planning Commission of India under the Chairmanship of Retd. Justice A.P. Shah ["**Justice A.P. Shah Report**"] examined the widespread directions for surveillance issued under the Telegraph Act and IT Act.

2013 The "International Principles on the Application of Human Rights to Communication Surveillance" ["**Necessary and Proportionate Principles**"], prepared by a coalition of Privacy Experts and Organisations, was launched at the U.N. Human Rights Council in Geneva.

25.09.2013 In response to an RTI request filed by 'SLFC.in', the Respondent No. 2 has stated that "on an average 7500 to 9000 orders for interception of telephones and 300 to 500 orders for interception of emails are issued by the Central Government every month."

11.02.2014 The Central Government, on the floor of Lok Sabha, admitted that the "Incidents of physical/electronic surveillance in the States of Gujarat and Himachal Pradesh, and the National Capital Territory of Delhi, allegedly without authorization have been reported. Union Cabinet has approved a proposal to set up a

Commission of Inquiry under Commission of Inquiry Act, 1952 to look into these incidents."

02.05.2016 Internet Freedom Foundation, the Petitioner No. 1 herein, was founded as a registered charitable Trust, setup *inter alia* to protect, promote and defend human rights of citizens using information communication technologies.

27.04.2017 This Hon'ble Court, in **Karmanya Singh Sareen v. Union of India,** S.L.P.(C) No. 804 of 2017. allowed the Petitioner-Trust's I.A. No. 4 of 2017 to intervene and assist on issues affecting privacy of Indian citizens using social media platforms, viz., WhatsApp and Facebook.

15.05.2017 The Hon'ble Constitution Bench was pleased to permit the Petitioner-Trust to make oral arguments in **Karmanaya Singh Sareen** (*supra*).

19.07.2017 In response to a question raised in Rajya Sabha, the Minister for State for Home Affairs stated that: "The Security/Intelligence agencies regularly monitor the popular social media sites and websites and take necessary action in case of they find any classified material or provocative material or anti-national or terror related material hosted / circulated on such sites."

27.06.2018 The 'Committee of Experts' constituted by the Union of India under the Chairmanship of Justice B. N. Srikrishna submitted their Report titled "A Free and

Fair Digital Economy: Protecting Privacy, Empowering Indians."

20.12.2018 The Central Government notified ten (10) security and intelligence agencies to carry out the interception, monitoring and decryption activities. The agencies included the Intelligence Bureau, Central Bureau of Investigation, and the Cabinet Secretariat (Research & Analysis Wing) that are beyond parliamentary or scrutiny or statutory oversight.

28.12.2018 The Petitioner-Trust, through its Executive Director, has sent queries Respondent No. 2 under the Right to Information Act, 2005, seeking a wide array of information relating to authorizations issued under Section 69 of the IT Act and Rules thereunder. The replies will shed further light on the current state of electronic surveillance in India.

08.01.2019 Hence, the present Writ Petition.

IN THE SUPREME COURT OF INDIA

CIVIL ORIGINAL JURISDICTION

(Under Article 32 of the Constitution of India)

WRIT PETITION (CIVIL) NO. OF 2019

IN THE MATTER OF:-

(1) INTERNET FREEDOM FOUNDATION
Through its Chairman,
E-215, Third Floor
East of Kailash, **PETITIONER NO. 1**
New Delhi - 110 065

(2) RAMAN JIT SINGH CHIMA
[redacted]
PETITIONER NO. 2

VERSUS

(1) UNION OF INDIA
Ministry of Law and Justice,
Department of Legal Affairs,
Through its Secretary,
4th Floor, A Wing,
Rajendra Prasad Road,
Shastri Bhavan,
New Delhi – 110 001 **RESPONDENT NO. 1**

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

(3) MINISTRY OF ELECTRONICS & INFORMATION TECHNOLOGY
Through the Secretary
Electronics Niketan,
6, CGO Complex,
Lodhi Road,
New Delhi – 110 003 **RESPONDENT NO. 3**

(4) MINISTRY OF COMMUNICATION
Through the Secretary
Department of Telecommunications
Sanchar Bhawan
20 Ashoka Road
New Delhi – 110 001 **RESPONDENT NO. 4**

A PETITION UNDER ARTICLE 32 OF THE CONSTITUTION OF INDIA FILED IN PUBLIC INTEREST

To,

The Hon'ble Chief Justice of India
and His Companion Judges of
the Hon'ble Supreme Court of India

The Humble Petition of the
Petitioner above named

MOST RESPECTFULLY SHOWETH

1. The present Writ Petition under Article 32 of the Constitution of India, filed in public interest, seeks to challenge the constitutional validity of Section 69 of the Information Technology Act, 2000 ["**IT Act**"] and The Information Technology (Procedure for Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 ["**2009 IT Rules**"] enacted pursuant to Section 69(2) read with Section 87(2)(y) of the Act, for being violative of Articles 14, 19(1)(a) and 21 of the Constitution. Consequently, the Petitioners seek a writ of *certiorari* or any other appropriate writ, order, or direction to quash the Notification dated 20.12.2018 (bearing No. 14/07/2011-T) ["**Impugned Notification**"], wherein ten (10) Security and Intelligence Agencies ["**Authorised Agencies**"] of the Central Government have been authorised to intercept, monitor, and decrypt [collectively as "**Electronic Surveillance**"] any information generated, transmitted, received, or stored in any computer resource. True Copy of The Information Technology

(Procedure for Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 is annexed herewith as **ANNEXURE P-1 (Page Nos. 69 to 83)**. True Copy of the Notification dated 20.12.2018 (bearing No. 14/07/2011-T) issued by the Ministry of Home Affairs is annexed herewith as **ANNEXURE P-2 (Page No. 84)**.

2. Internet Freedom Foundation ["**IFF**"], Petitioner No. 1 herein, is a registered charitable Trust, setup *inter alia* to protect, promote and defend human rights of citizens using information communication technologies ["**ICT**"]. The Petitioner-Trust is deeply concerned by the pervasive, sweeping, and clandestine activities of the State to intercept, monitor, and decrypt communications and other data generated, stored, shared, or transmitted through digital platforms. The existing legal regime governing electronic surveillance, specifically through the IT Act and Rules thereunder, have undermined the freedom of speech and expression of Internet users, and have adversely impacted the right to privacy of citizens. To this end, the Petitioners humbly state that the said provisions enabling electronic surveillance are illegal and unconstitutional, *inter alia,* for the following reasons:

A. Section 69 of the IT Act, impugned herein, gives overbroad, sweeping, and arbitrary powers to the State to conduct covert electronic surveillance by intercepting, monitoring, and decrypting digital communications. The very existence of such surveillance apparatus and authority with the State, regardless of its actual use, infringes fundamental rights under Articles 19(1)(a) and 21 of the Constitution. Surveillance impacts the right to privacy, especially "intellectual privacy" (the freedom to read and debate without being monitored). It chills the exercise of

liberties under Articles 19 and 21, and prevents people from thinking about, reading and exchanging unorthodox, controversial or provocative ideas. As explained by Justice Subba Rao in **Kharak Singh v Union of India,** [1964] 1 SCR 332, surveillance places psychological restraints that conditions an individual's mind and affects her freedom to think and express herself freely, in a way that impacts her personal liberty.

B. The constitutional standard applicable to adjudicating privacy violations is the proportionality standard, which has now been crystallised and elaborated in **K. S. Puttaswamy v. Union of India** (2017) 10 SCC 1 ["**Puttaswamy (*Privacy*)**"] and **K. S. Puttaswamy v. Union of India** (2018) 12 SCALE 1 ["**Puttaswamy (*Aadhaar*)**"]. Section 69(1) of the IT Act and the accompanying Rules and Notification fall foul of this proportionality and necessity standard.

C. Most importantly, the sub-clause (1) and (2) of Section 69 read with 2009 IT Rules lack any modicum of independence, impartiality, or application of judicial mind, and thus fail the test of adequate procedural safeguards. The present legal regime has vested the sole authority to authorise electronic surveillance to the Executive. Moreover, the authority to review such directions is entirely reserved in the hands of the Executive, without any parliamentary or judicial oversight. Consequently, the violation of fundamental rights of citizens is unilateral, leaving no recourse for aggrieved citizens to seek judicial review against arbitrary surveillance. The unquestioned discretion conferred upon the Executive is *ex-facie*

arbitrary, unreasonable, and undermines the concept of separation of powers.

D. The present legal framework governing electronic surveillance fails the test of proportionality, inasmuch as the provisions (viz., Section 69 and 2009 IT Rules) are open-ended and vague, creating a chilling effect on free expression of citizens. Most of the grounds specified under Section 69(1) to carry out electronic surveillance are a *verbatim* reproduction of restrictions contained in Article 19(2). Consequently, the Executive has an unguided discretion to justify electronic surveillance. Notably, the provision also encompasses circumstances relating to "defence of India," although such an expression is neither defined under the IT Act nor recognised under Article 19(2). Egregiously, the provision enables the State to conduct perpetual, untargeted, and mass surveillance of her citizens, under a pretext for "investigation of any offence".

E. While secrecy may be an inherent trait, and even the paramount objective for carrying out electronic surveillance, the IT Act and 2009 Rules have, while excessively delegating to the Executive, failed to instil adequate safeguards to prevent abusive, excessive, and arbitrary exercise of its powers. In particular, the "necessary or expedient" standard adopted under sub-clause (1) of Section 69 to authorise electronic surveillance woefully falls short of "the test of proportionality" - a *sine-qua-non* to curtail fundamental rights under Articles 19(1)(a) and 21.

3. At the outset, the Petitioners submit that the electronic surveillance regime is thoroughly incompatible with the spirit of directions issued by this Hon'ble Court in **People's Union for Civil Liberties v. Union of India** (1997) 1 SCC 301 ("**Wiretapping Judgment**"), in the context of rampant and illegal tapping of telephonic conversations under the Telegraph Act, 1885. In any event, the rapid growth of ICT and dangers it poses to civil rights, the safeguards guaranteed under the **Wiretapping Judgment** (*supra*) require to strengthened, or perhaps, reconsidered. Pertinently, the decisions of this Hon'ble Court in **Puttaswamy** (*Privacy*) and **Puttaswamy** (*Aadhaar*) have enumerated the evolving boundaries and safeguards necessary against violation of individual liberties and freedoms in the digital age. Justice Sanjay Kishan Kaul in **Puttaswamy** (*Privacy*) (*concurring*) aptly underscored the concerns of surveillance in the following words:

> "585. The growth and development of technology has created new instruments for the possible invasion of privacy by the State, including through surveillance, profiling and data collection and processing. Surveillance is not new, but technology has permitted surveillance in ways that are unimaginable. Edward Snowden shocked the world with his disclosures about global surveillance. States are utilising technology in the most imaginative ways particularly in view of increasing global terrorist attacks and heightened public safety concerns. One such technique being adopted by the States is "profiling". …"

4. To this end, the present Writ Petition raises several important questions of law involving interpretation of the Constitution. In particular, this Hon'ble Court has to examine:

(a) What is the standard for establishing an infringement of fundamental rights, and demonstrating "harm", in the context of State-enabled surveillance, which, by its very definition, involves a modicum of secrecy?

(b) Whether the standards laid down in the **Wiretapping Judgment** (*supra*) require to be updated in view of the proliferation of electronic and digital surveillance, in the modern world?

(c) Whether the existing legal regime under the IT Act, the 2009 IT Rules, and the impugned Notification, especially the lack of procedural safeguards and the overbroad nature of the provisions, conforms with the principle of proportionality, set out in **Puttaswamy** (*Privacy*) and **Puttaswamy** (*Aadhaar*)?

5. To best of our knowledge, there is no other Petition, either pending or disposed off, that has been filed before this Hon'ble Court or any other court challenging the constitutional validity of Section 69 of the IT Act and 2009 IT Rules. The Impugned Notification dated 20.12.2018 (bearing No. 14/07/2011-T) is already under challenge before this Hon'ble Court in W.P.(C) No. 02 of 2019 (**Amit Sahni v. Union of India**).

I. DESCRIPTION OF PARTIES

6. IFF, Petitioner No. 1 herein, is a registered under the provisions of Indian Trust Act, 1882 (bearing IN-DL44196137899619O). IFF is represented through its Chairman, Mr. Raman Jit Singh Chima, and is authorized to file the present Petition by virtue of the Resolution dated August 29, 2018. Voluntary contributions received by the Petitioner-Trust are exempt from levy of income

tax under Section 80G of Income Tax Act, 1961. Pertinently, the objectives of the Petitioner-Trust include:

> "(b) to create awareness among general public about the Constitution of India and the rights of citizens enshrined therein, human rights of all peoples, through campaigns, shows and other interactive medium;
>
> (j) to advocate and promote the use of open source software, encryption, security research, file sharing tools, civil liberties and a world of emerging technologies which further the values of the Constitution of India;
>
> (k) to advocate and defend freedom of speech, privacy, innovation, rights to access of information which furthers the freedom of speech and expression under the Constitution of India;
>
> (l) To provide legal assistance, support organisations in research and advocacy on the Trusts objects contained."

True Copy of Trust Deed of Petitioner No. 1 dated 02.05.2016 is annexed herewith as **ANNEXURE P-3 (Page Nos. 85 to 104)**.

7. The Petitioner-Trust was established on 02.05.2016 to secure the rights of Indian Internet users before policymakers, regulators, courts, and the wider public sphere. The founding members of the Petitioner-Trust were responsible for organising a public spirited campaign called "SaveTheInternet" in 2016 to prevent anti-competitive and abusive commercial practices of Internet companies and telecom operators. The "SaveTheInternet" campaign was led by a diverse section of activists, intellectuals, and professionals working on issues of civil rights, technology and policy related aspects of the Internet. The founders of the Petitioner-Trust started a signature campaign through an online platform called "SaveTheInterenet.in," which garnered over 1.2

million signatures to oppose rules and policies to curtail "network neutrality." The campaign led to enactment of Differential Tariff Regulations, 2016 by the Telecom Regulatory Authority of India ["**TRAI**"] to prohibit any discriminatory practices adopted by Internet companies and telecom operators affecting free and equal access to information and communications on the Internet. For a structured engagement, the volunteers of the "SaveTheInternet" campaign established IFF to work on issues of privacy, free speech, network neutrality, and innovation on the Internet.

A.	Authorised Person	:	Mr. Raman Jit Singh Chima Chairperson
[redacted]		[redacted]	
[redacted]		[redacted]	
D.	E-Mail & Tel.	:	trust@internetfreedom.in 011-41437971

8. The present Board of Trustees of the Petitioner No. 1 comprises of diverse and accomplished professionals, who are experts in field of Internet, law, public policy, and community engagement. The Trustees do not receive any remuneration for their service as trustees from the donations received by the Petitioner No. 1. The names and their professional expertise of the Trustees are given below:

No.	**Name**	**Profession**
1.	Apar Gupta Executive Director	Advocate & Policy Professional
2.	Aravind Ravi Sulekha	Engineer & Technologist
3.	Karthik Balakrishnan Co-Chair, IFF	Engineer & Technologist
4.	Rachita Taneja	Activist & Campaigner

5.	Raman Jit Singh Chima Chairperson, IFF	Advocate & Policy Professional
6.	Rohin Dharmakumar	Journalist & Startup Founder

9. In addition, the Petitioner-Trust has proactively intervened and assisted courts in India on cases affecting the rights of citizens for an open, equitable and secure access to the Internet. Notably:

(a) This Hon'ble Court, vide Order dated 27.04.2017, allowed the Petitioner-Trust's I.A. No. 4 of 2017 to intervene and assist in **Karmanya Singh Sareen v. Union of India,** S.L.P.(C) No. 804 of 2017. On 15.05.2017, the Hon'ble Constitution Bench was pleased to permit the Petitioner-Trust to submit oral arguments on the violation of privacy rights of Indian users by WhatsApp and Facebook. True Copy of the Order dated 27.04.2017 and 15.05.2017 in S.L.P.(C) No. 804 of 2017 passed by this Hon'ble Court are annexed herewith as **ANNEXURE P-4 (Page Nos. 105 to 107)** and **ANNEXURE P-5 (Page Nos. 108 to 110)**, respectively.

(b) The High Court of Delhi on 19.09.2016 issued notice to an application for impleadment in **Laksh Vir Singh Yadav v. Union of India,** W.P. (C) No. 1021 of 2016, a case related to the creation of the "Right to be Forgotten" in India. The Hon'ble High Court of Delhi was pleased to issue notice on the said application on 19.09.2016, and arguments on the intervention will be heard after pleadings are complete.

10. Besides interventions through courts, the Petitioner-Trust has actively engaged in public consultations held by TRAI, by submitting written responses and participating in stakeholder consultations. In addition, the Petitioner-Trust has provided expert inputs to the Parliamentary Standing Committees and

other authorities on policy related initiatives in the field. The Petitioner-Trust is currently at the forefront of public awareness and advocacy efforts in India to further privacy and data protection in India, through an innovation online campaign called "SaveOurPrivacy". Their efforts have been widely applauded and received endorsements from more than 11,388 individuals and 32 organisations from various walks of life, as on January 02, 2019.

11. Mr. Raman Jit Singh Chima, Petitioner No. 2 herein, is a C-Founder and the Chairperson of the Petitioner-Trust. Besides his voluntary work at IFF, he currently serves as a Policy Director at Access Now – an international non-profit organisation – working with its global policy team in protecting an open Internet and advancing the rights of users at risk across the world. He was also a founding volunteer with the SaveTheInternet.in net neutrality coalition. He has assisted the legal team involved in **Shreya Singhal v. Union of India** (2015) 5 SCC 1, arguing to struck down Section 66A of the IT Act as being violative of Articles 14 and 19(1)(a). He has been featured in Forbes Magazine's 30-Under-30 list of leaders in India under the Law and Policy category in 2016.

A. Full Name	:	Mr. Raman Jit Singh Chima Chairperson
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
D. E-Mail & Tel.	:	raman@internetfreedom.in 011 – 4986 9514

12. The Petitioners do not have any personal interest and are not filing the instant Petition for any private gain or oblique motive other than larger public interest. The Petition is being filed *bona*

fide in public interest for the benefit of Internet users and citizens of India. Since these persons are numerous, and unaware of directions given to conduct electronic surveillance of their communications under the impugned provisions, given the inherently secret nature of surveillance, they are unlikely to approach this Hon'ble Court. There is no civil, criminal or revenue litigation, involving the Petitioners, that is pending or decided in relation to issues raised in the present Writ Petition.

13. The Petitioners have not made any representation to the Respondents thus far, in view of the urgency involved and grave violation of fundamental rights. The Petition is based on authentic information and other public documents sourced from the Respondents. The Petitioners have means to pay costs, if any, imposed by the Hon'ble Court and on an undertaking to the Hon'ble Court in that respect.

14. **Union of India**, Respondent No. 1 herein, is represented through the Secretary of Department of Legal Affairs under the Ministry of Law & Justice in accordance with the Government of India (Allocation of Business) Rules, 1961. The Ministry of Law & Justice is responsible for defending cases relating to the constitutional validity of central legislations and rules before this Hon'ble Court.

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

16. **Ministry of Electronics, Information and Technology**, under the Central Government, is Respondent No. 3 herein, and is represented through its Secretary, is the nodal agency responsible for governing and implementing the provisions of the Information Technology Act, 2000 and Rules thereunder.

17. **Ministry of Communications, Dept. of Telecom,** under the Central Government, is Respondent No. 4 herein, and is represented through its Secretary, is the nodal agency responsible for governing and implementing the provisions of the Telegraph Act, 1885 and Rules thereunder.

II. LAWS GOVERNING SURVEILLANCE IN INDIA

18. Primarily, the special laws enacted by the Parliament relating to electronic surveillance are governed under:

(a) THE TELEGRAPH ACT, 1885: By virtue of Section 5(2), substituted vide Telegraph (Amendment) Act, 1972, the Central and State Governments have been conferred with lawful authority to intercept or detain messages transmitted through the 'telegraph'. Section 3(1AA) defines 'telegraph' as any "appliance, instrument, material or apparatus used or capable of use for transmission or reception of signs, signals, writing, images and sounds or intelligence of any nature by wire, visual or other electronic-magnetic emissions, radio waves or Hertzian waves, galvanic, electric or magnetic means." Section 5(2) reads as follows:

> (2) 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.

(b) THE INFORMATION TECHNOLOGY ACT, 2000: Section 69(1), impugned herein, authorises the Central and State Governments to monitor, intercept, or decrypt information contained in any 'computer resource'. A 'computer resource', defined under Section 2(1)(k), refers to a "computer, computer system, computer network, data, computer data base or software." The provision, as originally stood from the year 2000 till 05.02.2009, vested the powers to intercept any information on the 'Controller of Certifying Authorities'. By virtue of Information Technology (Amendment) Act, 2008 ['**2008 IT Amendment**'], the Parliament extended the powers under Section 69 to "monitor" and "decrypt" electronic communications. Moreover, the 2008 Amendment introduced two additional grounds (viz., 'defence of

India' and 'investigation of any offence') to cause electronic surveillance. Section 69(1), in its original and amended form, is represented below:

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

19. The key similarities and differences between the powers conferred under the Telegraph Act and IT Act include:

	TELEGRAPH ACT	IT ACT
Scope	Intercept or detain messages transmitted through a 'telegraph'	Intercept, monitor, and decrypt any information generated, transmitted, received or stored using a 'computer resource'
Who can Authorise?	Central or State Government, or any officer authorised on their behalf	Central or State Government, or any officer authorised on their behalf
When?	On occurrence of public emergency or in the interest of public safety	**NIL**
On grounds?	Sovereignty and integrity of India Security of the State Friendly relations with foreign states Public order Preventing incitement to the commission of an offence	Sovereignty or integrity of India Defence 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 Investigation of any offence
Exempted	Messages exchanged by accredited correspondents of the press are barred from interception or detention	**NIL**

20. The procedure to be followed for issuing valid orders or directions for surveillance has been prescribed by the Central Government by virtue of Sections 7(2)(b) and 87(2)(y) of the Telegraph Act and IT Act, respectively. In the case of Telegraph Act, the Central Government inserted Rule 419A to the Telegraph Rules, 1951 to lay down the procedure for interception of any message or class of messages transmitted through a telegraph. Likewise, the 2009 IT Rules, impugned herein, provides a detailed scheme for interception, monitoring, and decryption of information in any computer resource.

21. Pertinently, Rule 419A of the Telegraph Rules and the 2009 IT Rules are identical in several respects. Key aspects relevant for the present Petition are specified below:

	TELEGRAPH ACT	IT ACT
Competent Authority	Secretary of Home Department, and in unavoidable circumstance, the Joint Secretary	Secretary of Home Department, and in unavoidable circumstance, the Joint Secretary
Competent Authority, in case of emergency	Head or Second Senior Most officer of security and law enforcement agencies, at Central Level. Director General of Police or equivalent rank, at State and UT level.	Head or Second Senior Most officer of security and law enforcement agencies, at Central Level. Director General of Police or equivalent rank, at State and UT level.
Composition of Review Committee	At the Central Level: (a) Cabinet Secretary, Chairman (b) Secretary (Law) (c) Secretary (DOT)	Review Committee(s) constituted under Rule

	At the State/UT Level: (a) Chief Secretary, Chairman (b) Secretary (Law) (c) Secretary (Other than Home Dept.)	419A of the Telegraph Rules, 1951
Duration	Valid up to 60 days, unless revoked earlier	Valid up to 60 days, unless revoked earlier
Renewal	3 times (or up to 180 days)	3 times (or up to 180 days)
Retention of directions	6 months	6 months
Retention of records	2 months, from the date of discontinuation by the service provider	2 months, from the date of discontinuation by the intermediary or person in-charge of computer resources

II. BRIEF STATEMENT OF FACTS

22. In the past 45 years, since the introduction of Section 5(2) vide the Telegraph (Amendment) Act, numerous instances of excessive, arbitrary and abusive use of surveillance powers by the State has come to the fore. For the first time, this Hon'ble Court took serious cognizance on the widespread abuse of phone tapping under Section 5(2) of the Telegraph Act in **PUCL Wiretapping** (*supra*), referring to a CBI Report that found that:

> "21. Investigation has revealed the following lapses on the part of MTNL
>
> (i) In respect of 4 telephone numbers though they were shown to be under interception in the statement supplied by MTNL, the authorisation for putting the

number under interception could not be provided. This shows that records have not been maintained properly.

(ii) In respect of 279 telephone numbers, although authority letters from various authorised agencies were available, these numbers have not been shown in lists supplied by MTNL showing interception of telephones to the corresponding period. This shows that lists supplied were incomplete.

(iii) In respect of 133 cases, interception of the phones were done beyond the authorised part. The GM (O), MTNL in his explanation has said that this was done in good faith on oral requests of the representatives of the competent authorities and that instructions have now been issued that interception beyond authorised periods will be done only on receipt of written requests.

(iv) In respect of 111 cases, interception of telephones have exceeded 180 days' period and no permission of Government for keeping the telephone under interception beyond 180 days was taken.

(v) The files pertaining to interception have not been maintained properly.

22. Investigation has also revealed that various authorised agencies are not maintaining the files regarding interception of telephones properly. One agency is not maintaining even the logbooks of interception. The reasons for keeping a telephone number on watch have also not been maintained properly. The effectiveness of the results of observation have to be reported to the Government in quarterly returns which is also not being sent in time and does not contain all the relevant information. In the case of agencies other than IB, the returns are submitted to the MHA. The periodicity of maintenance of the records is not uniform. It has been found that whereas DRI keeps record

for the last 5 years, in case of IB, as soon as the new quarterly statement is prepared, the old returns are destroyed for reasons of secrecy. The desirability of maintenance of uni-return and periodicity of these documents needs to be examined."

A. Directions of this Hon'ble Court in Wiretapping Judgment

23. Following such egregious instances, revealed by the investigations conducted by the CBI, this Hon'ble Court was pleased to issue the following directions in **PUCL Wiretapping** (*supra*):

"35. We, therefore, order and direct as under:

1. An order for telephone-tapping in terms of Section 5(2) of the Act shall not be issued except by the Home Secretary, Government of India (Central Government) and Home Secretaries of the State Governments. In an urgent case the power may be delegated to an officer of the Home Department of the Government of India and the State Governments not below the rank of Joint Secretary. Copy of the order shall be sent to the Review Committee concerned within one week of the passing of the order.

2. The order shall require the person to whom it is addressed to intercept in the course of their transmission by means of a public telecommunication system, such communications as are described in the order. The order may also require the person to whom it is addressed to disclose the intercepted material to such persons and in such manner as are described in the order.

3. The matters to be taken into account in considering whether an order is necessary under Section 5(2) of the

Act shall include whether the information which is considered necessary to acquire could reasonably be acquired by other means.

4. The interception required under Section 5(2) of the Act shall be the interception of such communications as are sent to or from one or more addresses, specified in the order, being an address or addresses likely to be used for the transmission of communications to or from, from one particular person specified or described in the order or one particular set of premises specified or described in the order.

5. The order under Section 5(2) of the Act shall, unless renewed, cease to have effect at the end of the period of two months from the date of issue. The authority which issued the order may, at any time before the end of two-month period renew the order if it considers that it is necessary to continue the order in terms of Section 5(2) of the Act. The total period for the operation of the order shall not exceed six months.

6. The authority which issued the order shall maintain the following records:

(a) the intercepted communications,
(b) the extent to which the material is disclosed,
(c) the number of persons and their identity to whom any of the material is disclosed,
(d) the extent to which the material is copied, and
(e) the number of copies made of any of the material.

7. The use of the intercepted material shall be limited to the minimum that is necessary in terms of Section 5(2) of the Act.

8. Each copy made of any of the intercepted material shall be destroyed as soon as its retention is no longer necessary in terms of Section 5(2) of the Act.

9. There shall be a Review Committee consisting of Cabinet Secretary, the Law Secretary and the Secretary, Telecommunication at the level of the Central Government. The Review Committee at the State level shall consist of Chief Secretary, Law Secretary and another member, other than the Home Secretary, appointed by the State Government.

(a) The Committee shall on its own, within two months of the passing of the order by the authority concerned, investigate whether there is or has been a relevant order under Section 5(2) of the Act. Where there is or has been an order, whether there has been any contravention of the provisions of Section 5(2) of the Act.

(b) If on an investigation the Committee concludes that there has been a contravention of the provisions of Section 5(2) of the Act, it shall set aside the order under scrutiny of the Committee. It shall further direct the destruction of the copies of the intercepted material.

(c) If on investigation, the Committee comes to the conclusion that there has been no contravention of the provisions of Section 5(2) of the Act, it shall record the finding to that effect."

24. Almost a decade later, in 2007, the Central Government inserted Rule 419A to the Telegraph Rule, 1951 to codify the binding direction issued by this Hon'ble in **PUCL Wiretapping** (*supra*). Similarly, by virtue of the 2009 IT Rules, similar mechanism has been adopted for carrying out electronic surveillance. Notably,

the 2009 IT Rules, are not entirely in consonance with the binding directions issued by this Hon'ble Court in **PUCL Wiretapping** (*supra*), and are thus further inadequate. Some of the significant deviations are captured hereinbelow:

	GUIDELINES IN **PUCL WIRETAPPING** (*supra*)	2009 IT RULES
Lawful authority	1. An order for telephone-tapping in terms of Section 5(2) of the Act shall not be issued except by the Home Secretary, Government of India (Central Government) and Home Secretaries of the State Governments. <u>In an urgent case the power may be delegated to an officer of the Home Department of the Government of India and the State Governments not below the rank of Joint Secretary.</u>	Rule 3 empowers the Head or the second senior most officer of the Authorised Agencies, or persons equivalent to the rank of Inspector General of Police at State level, to authorise electronic surveillance in case of emergency.
Purpose of Review	9. (*a*) The Committee shall on its own, within two months of the passing of the order by the authority concerned, investigate whether there is or has been a relevant order under Section 5(2) of the Act. Where there is or has been an order, whether there has been any contravention of the provisions of Section 5(2) of	As per Rule 22, the role of Review Committee(s) is confined to recording "its findings whether the directions issued under rule 3 are in accordance with provisions of sub-section (2) of section 69" and if not, it "may" set them aside. The authority to conduct an

	the Act. (*b*) If on an investigation the Committee concludes that there has been a contravention of the provisions of Section 5(2) of the Act, it shall set aside the order under scrutiny of the Committee. It shall further direct the destruction of the copies of the intercepted material. (*c*) If on investigation, the Committee comes to the conclusion that there has been no contravention of the provisions of Section 5(2) of the Act, it shall record the finding to that effect.	investigation to verify the particulars forming the basis for such surveillance order has not been expressly conferred.
Record keeping	7. The use of the intercepted material shall be limited to the minimum that is necessary in terms of Section 5(2) of the Act. 8. Each copy made of any of the intercepted material shall be destroyed as soon as its retention is no longer necessary in terms of Section 5(2) of the Act.	Rule 23 mandates all records relating to electronic surveillance to be destroyed after six months, unless such information is necessary for any valid purpose. In case of intermediaries, such records must be destroyed within two months. However, the broad scope of the provision encompasses the

		contents of surveillance orders, including the person(s), computer resource(s), and grounds.

25. It is also pertinent to note that in **PUCL Wiretapping** (*supra*), the vires of the parent statute - Section 5(2) of the Telegraph Act of 1885 - that authorised phone-tapping, was not "seriously challenged".

B. Questionable Efficacy & Institutional Capacity under the Telegraph Rules & 2009 IT Rules

26. Based on information available in public domain, the Petitioners submit that the safeguards suggested by this Hon'ble Court in **PUCL Wiretapping** (*supra*) have not been effectively implemented by the Respondents and reveal a malice of inadequate institutional capacity and credible oversight on use of surveillance regulations. For example:

(a) At any given point of time, the Authorised Agencies maintain surveillance on a large number of telephones and electronic devices. According to a news report published in India Today on 20.12.2010, more than 6,000 telephones were under watch in New Delhi alone. The list included bureaucrats, military officials, corporates, journalist and NGOs. True Copy of article "The Secret World of Telephone Tapping" published on India Today on 20.12.2010 is annexed herewith as **ANNEXURE P-6 (Page Nos. 111 to 119)**.

(b) The Competent Authority receives and grants authorisation to a large number of surveillance requests. In response to

an RTI request filed by "SLFC.in" in 2013, the Respondent No. 2 has stated that "on an average 7500 to 9000 orders for interception of telephones and 300 to 500 orders for interception of emails are issued by the Central Government every month." True Copy of article titled "Surveillance – Is there a need for judicial oversight" dated 25.09.2013 is annexed herewith as **ANNEXURE P-7 (Page Nos. 120 to 124)**. True Copy of response issued by Respondent No. 2 on 25.05.2011 is annexed herewith as **ANNEXURE P-8 (Page No. 125)**. Given the large number of requests, it is highly improbable that the Competent Authority has adequate time and opportunity to make an effective assessment on alternative means of acquiring information.

(c) As noted by the Justice Srikrishna Committee (page 125), the Review Committee usually convenes once every two months, and has the "unrealistic task" of reviewing more than 15,000-18,000 surveillance orders in every meeting.

27. The above statistics raise serious alarm on the institutional capacity of the Competent Authority and the Review Committees to handle, authorise, and review surveillance requests. Egregiously, the Central Government has admitted on the floor of Parliament that the "Incidents of physical/electronic surveillance in the States of Gujarat and Himachal Pradesh, and the National Capital Territory of Delhi, allegedly without authorization have been reported. Union Cabinet has approved a proposal to set up a Commission of Inquiry under Commission of Inquiry Act, 1952 to look into these incidents." True Copy of the Reply from Minster of State for Home Affairs dated 11.02.2014 is annexed herewith as **ANNEXURE P-9 (Page Nos. 126 to 128)**. However, to the best of the Petitioners' knowledge,

no such Commission has been set up till date, and thus, practices of authorised/unauthorised surveillance continue to go un-noticed by the citizens.

C. Pervasive Use of Legal Processes to obtain User Data

28. On the other hand, the Authorised Agencies of the Central Government and law enforcement agencies at the State level have been frequently monitoring communications on the Internet. In response to a question raised in Rajya Sabha, the Minister for State for Home Affairs stated that: "The Security/Intelligence agencies regularly monitor the popular social media sites and websites and take necessary action in case of they find any classified material or provocative material or anti-national or terror related material hosted / circulated on such sites." True Copy of the reply of the Minister of State for Home Affairs in Rajya Sabha dated 19.07.2017 is annexed herewith as **ANNEXURE P-10 (Page No. 129)**.

29. Moreover, there has been a huge spike in the number of requests received from major Internet companies from the law enforcement agencies for seeking disclosure of personal data of its customers. The following chart, based on the publicly available Transparency Reports of these companies, reveals the total number of requests, along with individual accounts covered by such requests, received from the enforcement authorities in India 2017:

2017	**NO. OF REQUESTS**	**ACCOUNTS INVOLVED**
GOOGLE	97,838	1,70,608
FACEBOOK	22,024	31,014
TWITTER	576	1,431

At this juncture, it is clarified that the above requests do not correspondent to requests under Section 69 alone, but it represents the entire number of requests received from the governmental agencies under various legal provisions.

30. Furthermore, the Petitioner No. 1 through its Executive Director has sought a wide array of information relating to authorizations issued under Section 69 of the IT Act on 28.12.2018. Replies from Respondent No. 2 are awaited, and will shed further light on the state of surveillance. True Copy of the RTI Applications dated 28.12.2018 filed by the Petitioner No. 1 is annexed herewith as **ANNEXURE P-11 (Page Nos. 130 to 141)**.

D. Latest Developments

31. The 'Report by the Group of Experts' constituted by the Planning Commission of India under the Chairmanship of Retd. Justice A.P. Shah [hereinafter "**Justice A.P. Shah Report**"] examined the widespread directions for surveillance issued under the Telegraph Act and IT Act. To this end, the Report of Group of Experts dated 16.10.2012 has identified key lacunae in the existing procedure and rules to prevent harms to individual's right to privacy. The Report stated:

> "6.4. … The regime does not require judicial oversight or authorization, it is unclear which agencies are legally authorized to undertake interception/access, systematic access or proactive disclosure of communications and classes of data is not prohibited, agencies are not required to be transparent to the public regarding the effectiveness and cost of each intercept, interception/access **is permitted for even minor offenses,** there is no requirement for standardization of orders, there are no additional safeguards for when interceptions/access invade individual's privacy beyond the

> targeted subject, and the individual is never notified that an interception/access took place, even after the close of the investigation. Furthermore, the regime is silent on certain categories of data – such as location data. The differences between the regimes, and the policy gaps that exist, facilitate violations of privacy as broad interception/access is permitted to a wide category of information, during vague and changing circumstances, without adequate safeguards in place."

This Hon'ble Court in **Puttaswamy** (*Privacy*) has endorsed the recommendations made by the Group of Experts. True Copy of the Justice A. P. Shah Report dated 16.10.2012 is annexed herewith as **ANNEXURE P-12 (Page Nos. 142 to 216)**.

32. The absence of judicial mind, *ex-ante* or *post facto*, for carrying out electronic surveillance has been universally deprecated across developed and developing democracies. The "International Principles on the Application of Human Rights to Communication Surveillance" ["**Necessary and Proportionate Principles**"], prepared by a coalition of Privacy Experts and Organisations, launched at the U.N. Human Rights Council in Geneva in 2013, has pithily encapsulated the principle in the following words:

> "Principle 6: Competent judicial authority
>
> Determinations related to Communications Surveillance must be made by a competent judicial authority that is impartial and independent. The authority must be:
>
> (i) separate and independent from the authorities conducting Communications Surveillance;
>
> (ii) conversant in issues related to and competent to make judicial decisions about the legality of

> Communications Surveillance, the technologies used and human rights; and
>
> (iii) have adequate resources in exercising the functions assigned to them."

Justice Nariman in **Puttaswamy** (*Privacy*) (*concurring*) has recognised the importance of the above international development for securing, protecting and interpreting the scope of right to privacy in India. True Copy of the 'International Principles on the Application of Human Rights to Communications Surveillance' (May 2014) is annexed herewith as **ANNEXURE P-13 (Page Nos. 217 to 231)**.

33. More recently, the 'Committee of Experts' constituted in 2017 under the Chairmanship of Justice B. N. Srikrishna highlighted the importance of transparency, due process, and proportionality in the conduct of surveillance, especially in their manifestation of judicial oversight, in the following manner:

> "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."

The Committee went on to give the examples of Germany (where legislative oversight exists), U.K. (where judicial review exists), and South Africa (where some form of both exist) and pointed out that the data protection legislations in these countries

dovetailed with each substantive legislation relating to national security. The U.S. and Canada too, require judicial authorisation for interception. True Copy of the Report titled "A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians" (relevant excerpts) submitted by the Committee of Experts under the Chairmanship of Justice B. N. Srikrishna dated 27.06.2018 is annexed herewith as **ANNEXURE P-14 (Page Nos. 232 to 305)**.

34. It is respectfully submitted that these authoritative sources make it clear that the "procedural safeguards" limb of the broader proportionality enquiry – as set out in the judgment(s) in *Puttaswamy* – require judicial oversight of surveillance.

35. In the above premises, aggrieved by the legal provisions governing 'Electronic Surveillance' in India under the IT Act and Rules thereunder, the Petitioners prefer the present Writ Petition *inter alia* on the following grounds, which are urged in the alternative and without prejudice to one another:

GROUNDS

A. LEGAL INJURY AND HARM

I. **BECAUSE** there is no scope for an individual subjected to surveillance to approach a court of law, either prior to, or during or subsequent to, acts of surveillance, since the system itself is covert, especially where it relates to electronic surveillance based on the grounds specified in section 69(1), namely

> "in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing

incitement to the commission of any cognizable offence relating to above."

Where this is for the "investigation of any offence", the subject of a criminal investigation may, at best, gain knowledge of interception, decryption, monitoring etc. under the impugned provisions in the course of prosecution, presumably at a stage no earlier than the filing of the chargesheet. Even then, there would be little scope for redress since even if such action is illegal, the evidence gathered would remain admissible given extant principles laid down by this Hon'ble Court (E.g. **State (NCT of Delhi) v. Navjot Sandhu**, (2005) 11 SCC 600). Therefore, with little or no possibility of individuals detecting and complaining of legal injury, it is imperative for this Hon'ble Court to test the constitutionality of the surveillance system erected by the impugned provisions along with the impugned notification, especially since its very existence, in the absence of oversight, impacts the fundamental rights of citizens in the following manner: -

i. First and foremost, the very act of surveillance – taken on its own – infringes fundamental rights under Articles 19(1)(a) and 21. While the "harm" that surveillance causes cannot be quantified in a physical or tangible form, this Hon'ble Court has never insisted upon a showing of physical injury as a threshold requirement to demonstrate the violation of a fundamental right. The Petitioners respectfully submit that the very existence of a surveillance system impacts the right to privacy and chills the exercise of liberties under Articles 19 and 21, and prevents people from thinking about, reading and

exchanging unorthodox, controversial or provocative ideas. Regardless of whether or not a citizen knows that her email is being read by the government, the perceived danger, founded on reasonable suspicion that this may happen, itself impacts the citizen's ability to express, receive and discuss such ideas. This was explained by Justice Subba Rao in his dissenting opinion in **Kharak Singh v State of UP** (*supra*) subsequently upheld as correct in **Puttaswamy** (*Privacy*), as follows.

> "In an uncivilized society where there are no inhibitions, only physical restraints may detract from personal liberty, but as civilization advances the psychological restraints are more. effective than physical ones. The scientific methods used to condition a man's mind are in a real sense physical restraints, for they engender physical (1) [1950] S.C.R.88. fear channelling one's actions through anticipated and expected groves. So also the creation of conditions which necessarily engender inhibitions and fear complexes can be described as physical restraints. Further, the right to personal liberty takes in not only a right to be free from restrictions placed on his movements, but also free from encroachments on his private life."

ii. Second, in the absence of parliamentary or judicial oversight, electronic surveillance gives the Executive the power to influence both the subject of surveillance and all classes of individuals, which is particularly dangerous since the provision is agnostic with respect to the subject of surveillance. In other words, constitutional functionaries may be the subject

matter of electronic surveillance under the impugned provision, without any checks outside the executive wing of government. The very existence of such disproportionate power vesting with one wing of government would violate not only Part III of the Constitution, which impacts the vertical relationship between the citizen and the State; but would also impact the horizontal separation of power between the executive, legislature and judiciary. Based on the rulings in **Puttaswamy** (*Privacy*) and **Puttaswamy** (*Aadhaar*), judicial oversight would be the minimum requirement for this system to pass constitutional muster, as the judiciary alone is competent to decide whether it is proportionate and whether less onerous alternatives are available.

II. **BECAUSE** for the reasons elaborated below – i.e. the overbroad and vague nature of Section 69; the lack of any adequate safeguards; the impossibility of ensuring substantive due process, while deciding whether the decision to intercept, monitor, or decrypt was compliant with the Act and Rules; the absence of any *ex ante* or e*x post* parliamentary or judicial oversight; and the failure of the government to enact a privacy/data protection law – results in a chilling effect on the freedom of speech and movement under Article 19(1)(a) and Article 19(1)(d) of the Constitution. It has been recognised by this Hon'ble Court in a catena of judgments that it is the existence of concentrated and centralized State power, rather than its actual or potential use that creates the chilling effect and leads to psychological restraint on the ability of citizens to think freely. This induces a change in behaviour, that is further violative of Article 21 of the Constitution.

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

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

IV. **BECAUSE** this doctrine is well-accepted across the world. In **NAACP v Alabama** (357) US 449 (1958) the Supreme Court of the United States famously struck down compelled disclosure of the membership lists of a civil rights organisation (the NAACP), noting that the knowledge of surveillance would force politically unpopular or dissident individuals and groups into self-censorship.

V. **BECAUSE** the chilling effect caused by the operation of the surveillance framework in India, is best explained in the Justice Srikrishna Committee Report:

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

VI. **BECAUSE** the absence of any mechanism whereby a citizen is informed that they have been placed under surveillance, *post facto* or at any point in the future, further adds to this environment of uncertainty, where the behaviour of a citizen is modulated by the chilling effect on the broad sweep of surveillance practices, rather than any actual notice of their privacy being infringed.

B. EVOLUTION OF THE 'PROPORTIONALITY STANDARD' TO ASSESS THE VIOLATION OF PRIVACY AND OTHER FUNDAMENTAL RIGHTS, CAUSED BY A SYSTEM OF STATE SURVEILLANCE

VII. **BECAUSE**, while the 2009 IT Rules impugned herein, ostensibly flow from the standards and guidelines laid down in **PUCL Wiretapping** (*supra*), that standard needs to be updated in view of the circumstances of that case, the changed factual scenario twenty-two years later, and the evolution of subsequent jurisprudence. Partly, this is because **PUCL Wiretapping** (*supra*) dealt with phone

tapping, much before the age of large-scale interception and surveillance of electronic communication. As this Hon'ble Court recognised in **Puttaswamy** (*Privacy*), the age of big data and digital surveillance presents a unique and specific set of challenges, which are not easily reducible to the problems and issues faced in the brick-and-mortar world.

VIII. **BECAUSE** a majority of the judges in **Puttaswamy** (*Privacy*) endorsed the globally-operating "proportionality standards" - applied, broadly, by constitutional courts in jurisdictions such as the European Union, Canada, and South Africa - to gauge the constitutionality of restrictions on right to privacy, i.e. to ascertain the (a) legality, (b) legitimate goal, (c) proportionality and (d) procedural guarantees/safeguards of the impugned provision that has violated the right to privacy.

IX. **BECAUSE** the component of proportionality was further elaborated by the Constitution Bench decision of this Hon'ble Court in **Puttaswamy** (*Aadhaar*), which held that the following four sub-components of proportionality need to be satisfied before the validity of a law can be upheld (at Pr. 267 & 433):

> – A measure restricting a right must have a legitimate goal (legitimate goal stage) and it is designated for a proper purpose.
>
> – It must be a suitable means of furthering this goal (suitability or rationale connection stage), i.e. measures are undertaken to effectuate the limitation are rationally connected to the fulfilment of the purpose.

> – There must not be any less restrictive, but equally effective alternatives (necessity stage), i.e. there are no alternative less invasive measures.
>
> – The measure must not have a disproportionate impact on the right holder (balancing stage), i.e. there is a proper relation between the importance of achieving the aim and importance of limiting the right.

X. **BECAUSE** this is Hon'ble Court in **Puttaswamy** (*Privacy*) and **Puttaswamy** (*Aadhaar*) recognised, and endorsed, the privacy principles as elaborated in the Justice A.P. Shah Report which will be applicable in the present case to ascertain the *vires* of Section 69 of the IT Act. These privacy principles pertain to notice, choice and consent, collection limitation, purpose limitation, access and correction, non-disclosure of information, security of data, openness or proportionality as to the scale, scope and sensitivity to the data collected, and accountability.

XI. **BECAUSE** this Hon'ble Court in **Puttaswamy** (*Privacy*) and **Puttaswamy** (*Aadhaar*) also took note of the fundamental principles of data collection, processing, and storage that reflect the proportionality principle and also underpin the EU General Data Protection Regulation ["**EU GDPR**"]. These include:

> principle of lawfulness, fairness, and transparency: that personal data shall be processed lawfully, fairly, and in a transparent manner in relation to the data subject;
>
> principle of purpose limitation: that the personal data must be collected for specified, explicit, and legitimate purposes;

principle of data minimization: that processing must also be adequate, relevant, and limited to what is necessary; and

principle of accuracy: that data must be accurate and, where necessary, kept up to date

principle of storage limitation: that data is to be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;

principle of integrity and confidentiality: that data processing must be secure; and

principle of accountability: data controller is to be held responsible.

XII. **BECAUSE**, therefore, it is respectfully submitted that in the twenty years since the judgment in **PUCL Wiretapping**, there has been an evolution both in the understanding of the nature of harms caused by surveillance in the digital age, as well as a clearer understanding of the contours of the proportionality standard, and how this standard interacts with the specific manner in which surveillance infringes upon privacy and other fundamental rights. It is respectfully submitted – as demonstrated below – that Section 69 of the IT Act and the IT Rules do not comply with this standard.

XIII. **BECAUSE** the judgment in **PUCL Wiretapping** (*supra*), as is evident from a reading of Paragraphs 17 and 30 thereof, based its standards and guidelines upon existing jurisprudence dealing with what constitutes “just, fair, and reasonable” procedure established by law, which is the

touchstone on which infringement of Article 21 rights may be justified. However, reasonableness under Article 21 has evolved over the last twenty-two years, and has bent towards greater rights-protection, in the manner outlined herein.

C. **THE ACT AND RULES FAIL THE TEST OF PROCEDURAL SAFEGUARDS DUE TO THE ABSENCE OF ANY JUDICIAL OR INDEPENDENT OVERSIGHT**

XIV. **BECAUSE** the IT Act and the 2009 IT Rules do not provide for any judicial, parliamentary, or independent oversight mechanism over electronic surveillance conducted under the Act and the Rules, either at the *ex-ante*, *ex-post*, or the review stage.

a. ***Ex-ante* Stage**: Section 69(1) permits the electronic surveillance of any information generated, transmitted, received or stored in any computer resource *only* by the Executive, i.e. by "the Central Government or a State Government or any of its officers specially authorised by the Central Government or the State Government, as the case may be, in this behalf".

b. ***Ex-post facto* Stage**: Rule 3 of the 2009 Rules prescribes that the aforesaid directions under Section 69 can only be passed by an order "issued by the competent authority" (although in unavoidable circumstances, such orders may be issued by officers not below the rank of the Joint Secretary to the Government of India). Rule 2(d) of the 2009 Rules defines the "competent authority" as the (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. Thus, there is no provision for judicial/independent oversight prior to the authorisation of surveillance, which order can only be given by an Executive officer.

c. **Review** Stage: Rule 2(q) read with Rule 7 read with Rule 22 of the 2009 IT Rules requires that any directions issued under Rule 3 of the IT Rules have to be reviewed by the Review Committee set up under Rule 419A of the Telegraph Rules, which does not comprise any judicial/independent member. Under Rule 419A(16) of the Telegraph Rules, the Review Committee at the Centre comprises solely of members of the executive, namely the Cabinet Secretary; the Secretary to the Govt. of India, Legal Affairs; and Secretary to the Govt. of India, Ministry of Telecommunications. The decision taken by the Review Committee is final, is not subject to parliamentary or judicial oversight, and does not require hearing the concerned individual pre or post the decision to place them under surveillance.

XV. **BECAUSE** apart from the Telegraph Act and the IT Act (which contain almost identical provisions on review), there is currently no data protection or privacy law that would safeguard the privacy rights of Indian citizens.

XVI. **BECAUSE** the absence of judicial authorisation as a pre-condition (or, in cases involving an emergency, post-facto adjudication) for interception and surveillance renders the

Rules unconstitutional. This is because, by design, surveillance - which operates in secret - curtails the operation of Articles 32 and 226 of the Constitution, as a person who suspects that she is under surveillance, in many cases will have no way of proving it, and cannot therefore establish a breach in accordance with Articles 32 and 226, until that information is revealed. The effective exclusion of Articles 32 and 226 therefore entails that, for all practical purposes, the decision of the Executive on whether fundamental rights have been validly and reasonably infringed, is final. It is respectfully submitted that this violates the requirements of fairness and due process under Article 21, as well as the broader requirements of natural justice. For these reasons, the absence of any judicial/parliamentary/independent oversight of the decision taken by the Review Committee renders the relevant Rules unconstitutional.

XVII. **BECAUSE**, further, the denial of judicial scrutiny amounts to an effective denial of remedies under Article 21 of the Constitution. An individual under surveillance, by design, does not know that she is being surveiled, and cannot therefore challenge it as wrongful or illegal. In the absence of a judicial determination that surveillance meets the proportionality standards under Article 21, the lack of ability to approach the courts effectively entails the denial of the right itself. In other words, the very fact that, in a large number of cases, affected individuals will be unable to move the Court to enforce their rights under Article 21, requires that the infringement of those rights must be subject to judicial scrutiny.

XVIII. **BECAUSE** this Hon'ble Court in **Puttaswamy** (*Aadhaar*), despite noting that what is in the interest of national security may be a question of policy, struck down Section 33(2) of the Aadhaar Act on the ground that it did not provide for any independent (judicial) oversight of the important powers (of disclosure of identity information and authentication records of the Aadhaar number holder) given to the Joint Secretary, and did not adequately protect the interest of individuals, and was therefore, unreasonable, disproportionate, and unconstitutional.

XIX. **BECAUSE** the "Necessary and Proportionate Principles" endorsed by this Hon'ble Court in **Puttaswamy** (*Privacy*) stipulate that in this age of rapid technological changes, legality vis-a-vis communication surveillance requires laws that restrict the right to privacy to be subject to periodic review through a consultative legislative or regulatory process. In particular, Principle 6 of these Principles, referred to above, requires that determinations related to Communications Surveillance must be made by an impartial and independent competent judicial authority.

XX. **BECAUSE** the Srikrishna Committee specifically noted that the lack of legislative/statutory inter-branch oversight in India was "not just a gap that is deleterious in practice but, post the judgment of the Supreme Court in Puttaswamy, potentially unconstitutional" since it did not satisfy the tests of **Puttaswamy** *(Privacy)* that any restriction to the right to privacy must be by law; must be necessary and proportionate; and must promote a legitimate state interest. As stated above, the Srikrishna Committee also highlighted the importance of transparency, due process, and proportionality in the

conduct of surveillance, especially in the need for judicial oversight. Giving the examples of Germany, U.K., and South Africa, the Committee noted that executive review alone "is not in tandem" with comparative models of democratic nations. Keeping this in mind, the Committee recommended that the Central Government bring in a law that would "provide for both parliamentary oversight as well as judicial approval of all requests for non-consensual access to personal data." However, no such law exists currently.

D. SECTION 69 OF THE IT ACT AND THE IT RULES DO NOT SUBSTANTIVELY FULFIL THE PRINCIPLES OF PROPORTIONALITY

XXI. **BECAUSE** neither Section 69 of the IT Act, nor the 2009 IT Rules have codified the basic principles of necessity and proportionality, as required under the **Puttaswamy** (*Privacy*) and the privacy principles elaborated in the Justice A.P. Shah Report. Although Rule 8 requires the competent authority to consider alternative means of acquiring information and ensure that no "other reasonable means" exist to acquire the information, the IT Act and Rules are silent on the proportionality requirement.

a. This, in itself, runs against the proportionality standard, since this requires a determination not in respect of whether there is a less onerous means of achieving a particular government objective (covered under Section 69 of the IT Act) but whether there is an alternative way of acquiring the information. There is, therefore, an inherent assumption that the only possible means of achieving a particular objective (e.g. preventing incitement of a cognizable

offence) is the acquisition of information, which is incompatible with the proportionality test. In other words, Rule 8 assumes that the least onerous means of achieving one of the objective set out in Section 69 of the IT Act is the acquisition of private information which, in itself, run against the extant law on privacy as contained in **Puttaswamy** (*Privacy*).

b. This is apart from the fact that there is unchecked discretion given to the Competent Authority to determine the standards of necessity, proportionality, collection limitation, fairness, and data minimisation, such that only such amounts of data are intercepted, monitored, or decrypted, as is necessary/required for the limited, specific purpose of the competent authority. This renders the impugned provision and the Rules unconstitutional.

XXII. **BECAUSE**, the principle of necessity was also recognised by the Justice Srikrishna Committee, which clarified that processing of personal data by the State on non-consensual grounds (as in the case of surveillance) must be "strictly confined by necessity" and the "State should not collect personal data more than what is necessary for a legitimate [or stated] purpose". The Committee thus opined that "any systematic collection of data is to be preceded by an assessment of the extent to which data collection would be proportionate having regard to the legitimate purpose at hand." It is submitted that these principles of necessity and proportionality in the collection of personal data have been violated by Section 69 of the IT Act and the 2009 IT Rules, in that the Act and Rules, as framed, violate the doctrine of necessity, apart from violating the PUCL

guidelines, which require that "[t]he use of intercepted material shall be limited to the minimum that is necessary". The Act and Rules do not strictly lay down a rule of necessity with respect to either use or collection of information.

XXIII. **BECAUSE** the 2009 IT Rules, specifically Rules 10 and 25(2) do not comply with the principle of purpose limitation, except for the purpose of "investigation" (as specified in Rule 25(2)), inasmuch as there is no restriction on the use of data that is monitored, intercepted, decrypted, or disclosed by/to one of the notified agencies/Central/State Government by any of the other agencies or by the State or Central Government.

XXIV. **BECAUSE** under the 2009 IT Rules, there is no consequence of illegally intercepting, monitoring, or decrypting personal information, nor is there any mandatory requirement for setting aside such orders in case they do not adhere to the prescribed procedure and safeguards mandated under Section 69(2) read with the IT Rules. Under Rule 9 of the 2009 IT Rules, even if the Review Committee gives a finding that the directions issued under Rule 3 are not in accordance with Section 69(2) of the Act, it "may" (not shall) set aside these directions and issue orders for the destruction of the copies.

E. **ABSENCE OF DUE PROCESS**

XXV. **BECAUSE** the decision to intercept, monitor, decrypt or disclose information collected under Section 69 of the IT Act and the 2009 IT Rules lack any due process, and are thus unconstitutional. This Hon'ble Court in **Puttaswamy**

(*Privacy*) and in **Mohd. Arif v Supreme Court**, (2014) 9 SCC 737 held that a law would be amenable to challenge under Article 21 not only on the ground that the procedure which it prescribes is not fair, just and reasonable but also on the grounds that the substantive provisions of the law violate the Constitution and of violation of substantive due process.

XXVI. **BECAUSE** the 2009 IT Rules require that the Review Committee (comprising of Executive officers) meet at least once every two months and record its findings about whether the directions issued under Rule 3 are in accordance with Section 69(2). However, responses under the RTI Act (annexed herein) have revealed that the Central Government alone issues 7500 to 9000 orders of interception of telephones in a month, while around 500 orders are issued every month for interception of emails. As noted by the Justice Srikrishna Committee Report, "the Review Committee has an unrealistic task of reviewing 15000-18000 interception orders in every meeting, while meeting once in two months." It is thus clear that no proper application of mind can take place on every interception order, to determine if it is lawful or not.

F. **MANIFEST ARBITRARINESS**

XXVII. **BECAUSE** Section 69 of the Act ought to be struck down since it suffers from the vice of manifest arbitrariness, as it has been framed by the legislature capriciously, irrationally and without an adequate determining principle, even in comparison to Section 5(2) of the Telegraph Act.

XXVIII. **BECAUSE**, Section 69 of the IT Act is wider than even Section 5(2) of the Telegraph Act, rendering the provision liable to be struck down on grounds of void for vagueness

a. *First*, Section 69 of the IT Act permits the appropriate government to "intercept, monitor or decrypt" any information generated, transmitted, received or stored in any computer resource, without the prerequisite requirement of "public emergency" or "public safety" that is present in Section 5(2) of the Telegraph Act. This removes even the minimum modicum of safeguard present in the Telegraph Act.

b. *Second*, the IT Act widens the second-tier test under the Telegraph Act by providing for two additional grounds for surveillance, namely in the interest of the "defence of India" and the "investigation of any offence"; which grounds do not find any mention in Article 19(2) of the Constitution.

c. *Third*, Section 69(3) imposes an additional obligation on intermediaries, subscribers and persons in-charge of the computer resource to "extend all facilities and technical assistance" to the intercepting agency.

XXIX. **BECAUSE** Section 5(2) of the Telegraph Act requires a public emergency or an issue of public safety for the provision to even be triggered. Despite the fact that surveillance under the IT Act is not only comparable, but is perhaps more invasive than telephone tapping, there is no explanation for why this higher threshold of public

emergency/public safety is absent from Section 69 of the IT Act. This inexplicable difference in Section 5(2) of the Telegraph Act and Section 69 of the IT Act, in itself, is evidence that Section 69 of the IT Act is capricious and irrational (especially given the absence of judicial oversight), apart from being disproportionate, excessive and unreasonable.

XXX. **BECAUSE** as would be evident from the **Wiretapping judgment** (*supra*), the trigger requirement of a public emergency or public safety also brings in an element of transparency, as is evident from the extract below: -

> "28. Section 5(2) of the Act permits the interception of messages in accordance with the provisions of the said section. "Occurrence of any public emergency" or "in the interest of public safety" are the sine qua non for the application of the provisions of Section 5(2) of the Act. Unless a public emergency has occurred or the interest of public safety demands, the authorities have no jurisdiction to exercise the powers under the said section. Public emergency would mean the prevailing of a sudden condition or state of affairs affecting the people at large calling for immediate action. The expression "public safety" means the state or condition of freedom from danger or risk for the people at large. When either of these two conditions are not in existence, the Central Government or a State Government or the authorised officer cannot resort to telephone-tapping even though there is satisfaction that it is necessary or expedient so to do in the interests of sovereignty and integrity of India etc. In other words, even if the Central Government is satisfied that it is necessary or expedient so to do in the interest of the sovereignty and integrity of India or the security of the

> State or friendly relations with sovereign States or public order or for preventing incitement to the commission of an offence, it cannot intercept the messages or resort to telephone-tapping unless a public emergency has occurred or the interest of public safety or the existence of the interest of public safety requires. Neither the occurrence of public emergency nor the interest of public safety are secretive conditions or situations. Either of the situations would be apparent to a reasonable person."

However, in the absence of a public emergency and without there being an underlying interest of public safety, Section 69 allows surveillance under an impenetrable shroud, where there is no situation which is "apparent to a reasonable person". It is submitted that Section 69 of the IT Act and IT Rules of 2009, in general, lack any requirement for transparency and accountability inasmuch as the persons affected by wrongful interception of their private communications are never made aware of this. Without a public emergency / public safety requirement, there is no publicly discernible situation either which would serve to alert citizens that the government may be resorting to surveillance, or to serve as a publicly verifiable justification for surveillance.

XXXI. **BECAUSE**, in any event, the public emergency / public safety requirement may justify the narrow view taken regarding judicial oversight in the **Wiretapping judgment** (*supra*), but the complete absence of such a requirement under Section 69 of the IT Act renders judicial oversight virtually indispensable.

XXXII. **BECAUSE**, Section 69(1) of the IT Act does not contain even the bare minimum exception that is present in the proviso to section 5(2) of the Telegraph Act, which provides that 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 Section 5(2) of the Telegraph Act.

G. SECTION 69 OF THE IT ACT AND THE 2009 IT RULES ARE DISPROPORTIONATE, VAGUE, ARBITRARY, AND SUFFER FROM THE VICE OF EXCESSIVE DELEGATION

XXXIII. **BECAUSE** it is settled law, as noted by this Hon'ble Court in **Shreya Singhal v Union of India**, (2015) 5 SCC 1, that a law can be struck down as being void for vagueness. A vague law impermissibly delegates basic policy matters to other authorities for resolution on *ad hoc* and subjective basis', with the attendant dangers of arbitrary and discriminatory application. The void for vagueness doctrine requires that regulated parties should know what is required of them, so that they may act accordingly, which is not the case with the Act.

XXXIV. **BECAUSE** Section 69(1) of the IT Act permits both the Central and State governments to "intercept, monitor or decrypt" or "cause to be intercepted, monitored or decrypted" any information "generated, transmitted, received or stored" in any "computer resource" (as defined under Section 2(1)(k) of the IT Act), without providing any adequate safeguards to prevent the infraction of fundamental rights under Articles 19(1)(a) and 21 of the Constitution, and therefore is unconstitutional.

XXXV. **BECAUSE** the serious privacy harms entailed in surveillance require that there must be a threshold level of gravity before surveillance can be ordered. The phrase "investigation of *any* offence" militates against this requirement, and therefore vests disproportionate powers in the government. In this context, it is respectfully submitted that other statutes authorising a form of surveillance have taken gravity into account: for example, the Habitual Offenders Act stipulates both that the offence in question must be of a serious character, and must be committed repeatedly, before the surveillance-and-reporting requirements kick in. In addition, it is submitted that authorizing incursions into the private domain in the course of investigation is, traditionally, within the exclusive domain of the judiciary alone (akin to the judiciary's power to issue warrants for search and seizure of premises), and the fact that Section 69 of the IT Act can be deployed in the investigation of criminal offences without any judicial oversight whatsoever is contrary to the horizontal separation of powers established under the Constitution of India.

XXXVI. **BECAUSE** a cumulative reading of Section 69 of the IT Act along with the 2009 IT Rules reveals that they are overbroad, vague, and disproportionate. Rule 9 of the IT Rules envisages that the direction of interception, monitoring, or decryption shall be of "any information" generated, transmitted, received, or stored in any computer resource, as is sent to or from any "class of persons" or "relating to any particular subject". However, it does not provide any guidance the Executive on how these "class of persons" is to be determined, or what is the safeguard to ensure that the "class of persons" remains limited and does

not extend to an entire (religious/geographic etc.) section of the population. In this respect, it is respectfully submitted that, in **Puttaswamy** *(Privacy)*, it is made clear that bulk or "mass" surveillance is ruled out under the proportionality standard. In paragraph 70, while referring to the **PUCL (Wiretapping)** judgment, Chandrachud J. observed that: *"The requirements also mandate describing the nature and location of the facilities from which the communication is to be intercepted, the nature of the communication and the identity of the person, if it is known."*

XXXVII. **BECAUSE** this Hon'ble Court in **A.K. Roy v Union of India**, (1982) 1 SCC 271, a similarly broad expression - "supplies and services essential to the life of the community" - was struck down for over-breadth, in the absence of specific enumeration of the good and supplies.

XXXVIII. **BECAUSE** apart from the above restriction on any person or class of persons, there are no restrictions on the interception, decryption, monitoring or disclosure of information by executive officers, done without any targeting.

H. **THE IMPUGNED NOTIFICATION IS UNCONSTITUTIONAL**

XXXIX. **BECAUSE** the security and intelligence agencies that have been notified and authorised under the impugned notification to carry out the interception, monitoring and decryption activities, particularly the Intelligence Bureau, Central Bureau of Investigation, and the Cabinet Secretariat (Research & Analysis Wing) lack a statutory basis, and are therefore hit by the **Puttaswamy** standard. It

is now well settled that any infringement on the right to privacy has to be authorised by law. However, although the surveillance requires are sanctioned under the IT Act, the agencies that have been notified to carry them out are not authorised by law. Thus, to the extent that the impugned Notification authorises these agencies, it is further unconstitutional.

XL. **BECAUSE** section 69(1) of the IT Act requires that a direction can only be passed by the Central or State Government of "any of its officers" specially authorised by the Central or the State Government. However, Rule 4 of the 2009 IT Rules as well as the impugned Notification envisage action by entire "agenc(ies) of the government", which is ultra vires section 69(1). Thus, in extending the powers of interception, monitoring, and decryption to "agencies", beyond the remit of "authorised officers" mentioned in Section 69(1), the 2009 IT Rules and the Impugned Notification are unconstitutional.

36. The Respondents are 'State' within the meaning of Article 12 of the Constitution and amenable to the writ jurisdiction of this Hon'ble Court.

37. The Petitioners have not filed any other petition before this Hon'ble Court or in any High Court or this Hon'ble Court for similar reliefs.

38. The Petitioners crave leave of this Hon'ble Court to add, alter or amend all or any of the above grounds at the time of hearing of the present Petition.

39. The Petitioners submits that there is no other equal or efficacious alternative remedy available to them.

40. The Petitioners state that they are approaching this Hon'ble Court as expeditiously as possible and there is no delay or laches in filing the present Petition.

41. This Hon'ble Court has jurisdiction to entertain try and dispose of this Petition under Article 32 of the Constitution of India.

PRAYER

In the premises, it is most respectfully prayed that this Hon'ble Court may be pleased to -

A. Issue a writ of *Mandamus* or any other appropriate writ, declaration, or order to declare Section 69 of the Information Technology Act, 2000 as ultra vires Articles 14, 19(1)(a), 19(1)(d), and 21 of the Constitution of India;

B. Issue a writ of *Mandamus* or any other appropriate writ, declaration, or order to declare The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 as ultra vires Articles 14, 19(1)(a), 19(1)(d), and 21 of the Constitution of India;

C. Issue a writ of *Certiorari* or any other appropriate writ, order, or directions to quash the Impugned Notification dated 20.12.2018 issued by Ministry of Home Affairs in exercise of powers under Section 69(1) read with Rule 4 of the IT Act and Rules thereunder as illegal, and violative of Articles 14, 19(1)(a), 20, and 21 of the Constitution of India, and thereby permanently restraining the Respondents/their authorities/ agents and the agencies authorised under Impugned Notification dated 20.12.2018 from enforcing the Notification;

D. Issue a Writ of Declaration and *Mandamus* or any other appropriate Writ, Direction, Order or such other appropriate remedy to do complete justice in the facts and circumstances of this present Writ Petition.

DRAWN BY Ms. Vrinda Bhandari, Advocate
Mr. Gautam Bhatia, Advocate
Mr. N. Sai Vinod, Advocate

FILED BY:

ADVOCATE FOR THE PETITIONERS
PRATEEK CHADDHA

DRAWN ON : 03.01.2019
FILED ON : 08.01.2019

APPENDIX – A

TELEGRAPH ACT, 1885

5. Power for Government to take possession of licensed telegraphs and to order interception of messages.—

(1) 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 authorized in this behalf by the Central Government or a State Government may, if satisfied that it is necessary or expedient so to do, take temporary possession (for so long as the public emergency exists or the interest of the public safety requires the taking of such action) of any telegraph established, maintained or worked by any person licensed under this Act.

(2) 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 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.

APPENDIX – B

INFORMATION TECHNOLOGY ACT, 2000

Until *Feb. 05, 2009*

69. Directions of Controller to a subscriber to extend facilities to decrypt information.

(1) If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource.

(2) The subscriber or any person incharge of the computer resource shall, when called upon by any agency which has been directed under sub-section (1), extend all facilities and technical assistance to decrypt the information.

(3) The subscriber or any person who fails to assist the agency referred to in sub-section (2) shall be punished with an imprisonment for a term which may extend to seven years.

With effect from Feb. 05, 2009

69 Powers to issue directions for interception or monitoring or decryption of any information through any computer resource

(1) Where the central Government or a State Government or any of its officer specially authorized by the Central Government or the State Government, as the case may be, in this behalf may, if is 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 relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may, subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information transmitted received or stored through 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 which has been directed under sub section (1), extend all facilities and technical assistance to -

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

(b) intercept or 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 an imprisonment for a term which may extend to seven years and shall also be liable to fine.

APPENDIX – C

G.S.R. 193 (E).— 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) These rules may be called the Indian Telegraph (Amendment) Rules, 2007.

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

(3) In the Indian Telegraph Rules, 1951, after rule 419, the following rule shall be substituted, namely:—

Rule 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. 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 authorized 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 message 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 authorized security i.e. 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. 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 the designated officers of the licensee(s) who have been granted licenses under Section 4 of the said Act, in writing by an officer not below the rank of Superintendent of Police or Additional Superintendent of Police or the officer of the equivalent rank.

(8) The officer authorized to intercept any message or class of message 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 agencies shall designate one or more nodal officers 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 requisitions for interception to the designated officers of the concerned service providers to be delivered by an officer not below the rank of Sub-lnspector of Police.

(10) The service providers shall designate two senior executives 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 officers of the service providers shall issue acknowledgment letters to the concerned 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 officers of the service providers shall forward every fifteen days a list of interception authorizations 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 authorizations. The list should include details such as the reference and date of orders of the Union Home Secretary or State Home Secretary, date and time of receipt of such orders and the date and time of Implementation of such orders.

(14) The service providers shall put in place adequate and effective internal checks to ensure that unauthorized 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 are responsible for actions for their employees also. In case of established violation of license conditions pertaining to maintenance of secrecy and confidentiality of information and unauthorized interception of communication, action shall be taken against the service providers as per Sections 20, 20-A, 23 & 24 of the said Act, and this shall include not only fine but also suspension or revocation of their licenses.

(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:

(a) Cabinet Secretary—Chairman

(b) Secretary to the Government of India Incharge, Legal Affairs — Member

(c) 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:

(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. 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 authorized security and Law Enforcement Agencies every six months unless these are, or likely to be, required for functional requirements.

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

ANNEXURE P-1

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 an 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 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;

(p) "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 or in combination with any other instrument, device, equipment or apparatus, to view or to inspect or listen to or record any information;

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

3. **Direction 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 Joint Secretary of 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 generation, transmitted, received or stored in any computer resource is not feasible,

the interception or monitoring of 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 in 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 for 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.

9. **Direction of interception or monitoring or decryption of any specific information.—** The direction of interception or monitoring or decryption of any information generation,

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 facilitates, 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.— 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

generation, 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.

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 of the method by which such copies, including corresponding electronic records 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 the 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 no 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 issues 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.

(2) Save as otherwise required for the purpose of any ongoing investigation, criminal complain 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 of 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 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.

TRUE COPY

ANNEXURE P-2

MINLSTRY OF HOME AFFAIRS

(CYBER AND INFORMATION SECURITY DIVISION)

ORDER

New Delhi, the 20th December, 2018

S.O. 6227(E).—In exercise of the powers conferred by sub-section (1) of section 69 of the Information Technology Act, 2000 (21 of 2000) read with rule 4 of the Information Technology Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, the Competent Authority hereby authorises the following Security and Intelligence Agencies for the purposes of interception, monitoring and decryption of any information generated, transmitted, received or stored in any computer resource under the said Act, namely:—

(i) Intelligence Bureau;
(ii) Narcotics Control Bureau;
(iii) Enforcement Directorate;
(iv) Central Board of Direct Taxes;
(v) Directorate of Revenue Intelligence;
(vi) Central Bureau of Investigation;
(vii) National Investigation Agency;
(viii) Cabinet Secretariat (RAW);
(ix) Directorate of Signal Intelligence (For service areas of Jammu & Kashmir, North-East and Assam only);
(x) Commissioner of Police, Delhi.

[No.14/07/2011-T]
RAJIV GAUBA. Union Home Secy.

TRUE COPY

ANNEXURE P-4

ITEM NO.501 COURT NO.2 SECTION XIV

S U P R E M E C O U R T O F I N D I A
RECORD OF PROCEEDINGS

Petition(s) for Special Leave to Appeal (C) No.804/2017

(Arising out of impugned final judgment and order dated 23/09/2016 in WPC No. 7663/2016 passed by the High Court of Delhi at New Delhi)

KARMANYA SINGH SAREEN AND ANR Petitioner(s)

VERSUS

UNION OF INDIA AND ORS Respondent(s)

(With appln. (s) for directions and intervention)

Date : 27/04/2017 This petition was called on for hearing today.

CORAM :
HON'BLE MR. JUSTICE DIPAK MISRA
HON'BLE MR. JUSTICE A.K. SIKRI
HON'BLE MR. JUSTICE AMITAVA ROY
HON'BLE MR. JUSTICE A.M. KHANWILKAR
HON'BLE MR. JUSTICE MOHAN M. SHANTANAGOUDAR

For Petitioner(s) Mr. Harish N. Salve, Sr. Adv.
Ms. Madhavi Divan, Adv.
Mr. Prabhas Bajaj, Adv.
Mr. T. Singh Dev, Adv.
Mr. Vikshit Arora, Adv.
Ms. Surubhi Mehta, Adv.
Mr. Gaurav Sharma, AOR
Mr. Tarun Verma, Adv.
Ms. Amandeep Kaur, Adv.

For Respondent(s) Mr. Tushar Mehta, ASG
Mr. A.K. Sanghi, Sr. Adv.
Ms. Vibha Datta Makhija, Sr. Adv.
Ms. Sadhna Sandhu, Adv.
Ms. Disha Vaish, Adv.
Ms. Swarupama Chaturvedi, Adv.
Mr. Vijay Prakash, Adv.
Mr. G.S. Makker, Adv.
Mr. Rajat Nair, Adv.

For R-2, 3 & 4 Mr. Kapil Sibal, Sr. Adv.
Mr. K.K. Venugopal, Sr. Adv.
Mr. Sidharth Luthra, Sr. Adv.
Mr. Tejas Karia, Adv.
Mr. Vivek Reddy, Adv.
Ms. Richa Srivastava, Adv.
Mr. Akhil Anand, Adv.
Mr. Shashank Mishra, Adv.
Mr. Arpit Gupta, Adv.
Mr. Koshy John, Adv.
Ms. Chanranya, Adv.
Ms. Tara Narula, Adv.
Mr. Ankur Talwar, Adv.
Mr. S. S. Shroff, AOR

For Intervenor Mr. K.V. Vishwanathan, Sr. Adv.
Ms. Vrinda Bandari, Adv.
Mr. Nikhil Nayyar, Adv.
Mr. T.V.S. Raghavendra Sreyas, Adv.
Mr. N. Sai Vinoda, Adv.
Mr. Mukunda Rao, Adv.
Mr. Ravi Raghunath, Adv.

For R-5 Mr. Sanjay Kapur, AOR
Mr. Anmol Chandan, Adv.
Ms. Megha Karnwal, Adv.
Ms. Shubhra Kapur, Adv.

UPON hearing the counsel the Court made the following

O R D E R

I.A. No.4 of 2017

This is an application for intervention filed by the Internet Freedom Foundation (IFF).

Having heard Mr. K.V. Vishwanathan, learned senior counsel for the applicant, the application for intervention stands allowed.

S.L.P.(C) No.804 of 2017

In pursuance of our earlier order, Mr. Harish N. Salve, learned senior counsel has filed certain questions of law. The same are taken on record.

Mr. Kapil Sibal, learned senior counsel appearing for the respondent No.2, WhatsApp, undertakes to file a set of propositions by tomorrow (28.04.2017).

Mr. K.K. Venugopal, learned senior counsel appearing for the respondent No.3, Facebook Inc., has filed an interlocutory application that relates to maintainability. Needless to say, the issue of maintainability shall be dealt with along with the main prayer.

Mr. Tushar Mehta, learned Additional Solicitor General has submitted that the Union of India is weeded to the principle of protecting individual freedom of the citizens and, accordingly, he will put forth his arguments.

Let the matter be listed at 10.30 a.m. on 15th May, 2017.

(Chetan Kumar)
Court Master

(H.S. Parasher)
Court Master

TRUE COPY

ANNEXURE P-5

ITEM NO. 501 COURT NO.2 SECTION xiv

S U P R E M E C O U R T O F I N D I A

RECORD OF PROCEEDINGS

Petition(s) for Special Leave to Appeal (C) No(s). 804/2017

(Arising out of the judgment dated 23.9.2017 in Writ Petition (C) No.7663 of 2016 passed by the High Court of Delhi at New Delhi)

KARMANYA SINGH SAREEN AND ANR. Petitioner(s)

VERSUS

UNION OF INDIA AND ORS. Respondent(s)

Date : 15/05/2017 This petition was called on for hearing today.

CORAM : HON'BLE MR. JUSTICE DIPAK MISRA
HON'BLE MR. JUSTICE A.K. SIKRI
HON'BLE MR. JUSTICE AMITAVA ROY
HON'BLE MR. JUSTICE A.M. KHANWILKAR
HON'BLE MR. JUSTICE MOHAN M. SHANTANAGOUDAR

For Petitioner(s) Ms. Madhavi Divan, Adv.
Mr. T. Singhdev, Adv.
Mr. Gaurav Sharma, AOR
Mr. Prabhas Bajaj, Adv.
Ms. Surbhi Mehta, Adv.
Ms. Amandeep Kaur, Adv.
Mr. Tarun Verma, Adv.
Ms. Nidhi Khanna, Adv.

For Respondent(s) Mr. Sanjay Kapur, AOR
Ms. Megha Karnwal, Adv.
Ms. Shubhra Kapur, Adv.
Mr. Kapil Sibal, Sr. Adv.
Mr. K.. Venugopal, Adv.
Mr. Sidharth Luthra, Sr. Adv.
Mr. Tejas Karia, Adv.
Mr. Vivek Reddy, Adv.
Ms. Richa Srivastava, Adv.
Mr. Shashank Mishra, Adv.
Mr. Arpit Gupta, Adv.
Mr. Ashwin Reddy, Adv.

Ms. Charanya, Adv.
Ms. Tara, Adv.
Mr. Koshi John, Adv.
Mr. Ankur Talwar, Adv.

Ms. Mayuri Tiwari, Adv.
Mr. S.S. Shroff, AOR

Mr. Tushar Mehta, ASG
Ms. Vibha Datta Makhija, Sr. Adv.
Mr. A.K. Sanghi, Sr. Adv.
Ms. Swarupama Chaturvedi, Adv.
Mr. Rajat nair, Adv.
Mr. Vijay Prakash, Adv.
Ms. Sadhana Sandhu, Adv.
Ms. Ranjita Rohatgi, Adv.
Ms. Anisha Mathur, Adv.
Mr. Gurmeet Singh Makker, AOR

Mr. K.V. Vishwanathan, Sr. Adv.
Ms. Vrinda Bhandari, Adv.
Mr. Abhishek Kaushik, Adv.
Mr. Ravi Raghunath, Adv.
Mr. A.M. Rao, Adv.
Mr. N. Sai Vinod, Adv.

UPON hearing the counsel the Court made the following

O R D E R

It is submitted by Ms. Madhavi Divan, learned counsel appearing for the petitioners that Mr. Harish Salve, learned senior counsel who had assured this Court to argue the matter today is busy before the International Court of Justice defending India and, therefore, the matter may be argued in his absence.

We accept the aforesaid submission. We permitted Mr. K.V. Vishwanathan, learned senior counsel who is supporting the cause of the petitioners to argue the matter. Ms. Madhavi Divan, learned counsel assisted him and also participated in the course of arguments.

After Mr. Vishwanathan, learned senior counsel submitted his arguments, we are obliged to note that Mr. K.K. Venugopal, learned

senior counsel had initially raised the issue of maintainability of the writ petition and, therefore, we permitted him to argue the same. He has commenced his arguments.

Let the matter be listed for further hearing at 10.30 a.m. on 16.5.2017.

WP (C) No. 347 of 2017

On being mentioned, the matter is taken on Board.

List the matter on 16.5.2017 along with SLP (C) No.804/2017.

(Gulshan Kumar Arora)
Court Master

(H.S. Parasher)
Court Master

TRUE COPY

ANNEXURE P-6

INDIA TODAY

The Secret World of Phone Tapping

Your private conversations can be easily monitored by the Government. How it is done, who's in charge, and the future.

Sandeep UnnithanBhavna Vij-AuroraAshish Khetan
December 20, 2010

ISSUE DATE: December 20, 2010
UPDATED: December 20, 2010 00:00 IST

Over a million mobile phones, across service providers, are under the surveillance of Central agencies in India through the year. Officially, the Government will admit to over 6,000 telephones in New Delhi being tapped. This secret hot list has as many as 400 bureaucrats and military officials monitored on suspicion of corruption, 200 corporate honchos, over 50 top journalists, an equal number of fixers, a dozen arms dealers, two dozen NGOs and about 100 high society pimps, drug dealers and hawala operators. This is in addition to suspected militants, their supporters and sympathisers and known criminals.

In an attempt to widen its surveillance net, the Home Ministry has now sought suitable amendments to the Indian Telegraph Act, 1885, to allow active intervention for tapping phones and monitoring Internet communication. Home Secretary G.K. Pillai says the home ministry is pursuing changes to the country's telecom laws to bring clarity in the Government's authority to intercept highly secure corporate communications. This will be part of broader changes related to lawful intercept policy and privacy.

Everyday, Pillai, the sole authoriser of such Central wiretaps, receives hundreds of fresh written requests for electronic surveillance. A majority of requests emanate from the Intelligence Bureau (IB), Income Tax Department, Central Bureau of Investigation (CBI), Directorate of Revenue Intelligence (dri) and the Enforcement Directorate (ED). Additional requests also come from state agencies who need the home ministry's permission to intercept phones in Union Territories. Law enforcement agencies can tap a phone without the home secretary's permission for the first week. Thereafter, a tap can be done only after a strong case is

made. In reality, a weak argument works. Crime and terrorism are the familiar rationales but they leave the door open for multi-level abuse. Each state has an average of 2,000 to 3,000 phones under surveillance at any given time.

Phone tapping is uncoordinated. Various agencies monitor numbers in silos. At times, a single number is simultaneously being monitored by multiple agencies of the state and Centre. The proliferation of off-the-shelf sophisticated listening devices and absence of a Central database compound the problem. Except in certain special laws, wiretaps can be used only as corroborative evidence in courts. But it is so easily done with such little effort that it becomes the first recourse for law enforcement authorities. With an increasing reliance on phone tapping as operational tools, the surveillance society is only set for consolidation.

Activists argue for a US-like system where only a judge authorises wiretaps after reviewing the evidence. "Civil liberties are far too important to be left to the executive or the home secretary. There is every danger of wrong permissions being given out, resulting in indiscriminate tapping," says former chief justice Rajinder Sachar.

Phone tapping is allowed under the general provisions of Section 5 of the Indian Telegraph Act, but only in "public emergency, or in the interest of public safety". In 1997, the Supreme Court, in response to a petition filed by justice Sachar, laid down five precepts for intercepting conversations-in the interests of national sovereignty and integrity, state security, friendly relations with foreign states, public order or for preventing incitement to the commission of an offence. "Tapping phones especially for tax evasion and corruption needs to be done only in the rarest of rare cases," says former ips officer-turned-lawyer Y.P. Singh.

There are seven Central agencies authorised to tap telephones-the IB, ED, Delhi Police, CBI, DRI, Central Economic Intelligence Bureau and the Narcotics Control Bureau. "Phone tapping is a legal instrument. It should be kept in safe custody of the court or very few officers should have access to it. Leaking tapes are like leaking official secrets; it not only adversely affects an individual but is also harmful to investigations and the prosecution process," says Arun Bhagat, former director, IB.

Often a hint of suspicion can put you under the scanner. Home ministry officials became suspicious of the flamboyant lifestyle of IAS officer Ravi Inder Singh. The bureaucrat shunned his official accommodation in favour of a plush guesthouse provided by his friend and co-accused Vinit Kumar. Singh's phones were kept under observation where he was heard referring to "Ukranian and Russian software", a code for prostitutes. Hotels were referred to as hardware and bribes were called laddoos. He was charged with giving clearance to a US-based telecom company, Telecordia, for mobile number portability. Dozens of other bureaucrats are believed to be under surveillance for similar reasons. But for every legal case, there are hundreds of illegal wire taps. Five years ago, a Mumbai newspaper publicised explicit phone conversations of actor Salman Khan. The Government claimed the

voice on the tapes was not Khan's. It was a cover-up of an illegal wiretap. The conversations had been leaked out from the city crime branch. Four private detectives were arrested for illegally obtaining phone records of former Samajwadi Party leader Amar Singh in 2005.

But what if an illegally monitored phone yields evidence of wrongdoing? Officials say a backdated application is sought from the home secretary.

Every agency fills out an authorisation slip before placing a phone under surveillance. In the states, it is the state home secretary who signs this. Officially, telephones of politicians cannot be tapped-a qualifier on the slip says the surveilled person is not an elected representative. Before the advent of cellular phones, state agencies often strung out parallel lines from telephone poles, rented lodgings in the vicinity or even pitched a tent in the vicinity posing as nomadic tribes. Often the target would get to know due to the disturbance in the phone. Calls could only be listened to, not recorded. Cellphones gave organised crime syndicates mobility and anonymity as connections could be bought in fake names. In the mid-1990s, operators were ill-equipped to intercept calls. In the first instance of surveillance, the then deputy superintendent of the Uttar Pradesh Special Task Force (stf) Rajesh Pandey got a telecom engineer in Allahabad to devise a typewriter-sized interception box. The box was lugged around and connected to switching stations.

Today, every cellular service provider has an aggregation station which is a clutch of servers called mediation servers (because they mediate between the cellular operators and the law enforcement agencies) to intercept phones. Two kinds of interception facilities are available-Integrated Services Digital Network (ISDN) and the leased line. Under ISDN, a mediation server intercepts a call, and then transmits it through a Primary Rate Interface (PRI) line to the office of a government

agency. The police can listen to the phone on their PRI line and store the recording to attached computers. Simultaneously, a sound file of the intercepted call is also recorded and stored in the mediation server. In ISDN, the transfer of call-related data doesn't happen in real time. A slow 64 kbps speed results in a time lag of two to three minutes. Data packets are lost in traffic and calls don't reach the PRI line.

Under the leased line facility, the service provider gives the agency direct access to its backbone network through a dedicated fast speed fibre optic cable connection. The call-related data is not only transmitted in real time, at the lightning speed of 2 mbps, the chances of missing any call are minimal. But since the cost of laying a fast-speed fibre optic cable connection is higher, state agencies are more dependent on ISDN. For instance, the Mumbai Crime Branch has leased line connections from just three service providers, for the rest it uses ISDN. At any given point of time a service provider can provide a maximum of eight agencies the call interception facility to a given number.

The commonest surveillance methods are sourcing an individual's call data records (CDR) or list of numbers dialled and received. This does not require government sanction. Fed into a special software, the CDR rapidly builds up a 'relationship tree' or charts the relationship between thousands of calls. This can easily be used to pry on civilians. A secretary in a Central ministry is believed to source the CDRs of journalists to trace their sources.

Technology is an antidote to privacy. The rich and the famous do try and escape it. In one of her taped conversations, Niira Radia instructs Tamil Nadu Chief Minister M. Karunanidhi's wife Rajathi's charted accountant to call on her Tata Docomo number. Since lawful intercept of a cellphone can only be done by writing to the concerned telecom service provider, Radia evidently felt secure on a number provided by

her client, Tata. Not surprisingly, Radia's Idea and MTNL numbers only were intercepted. Anil Ambani's aide Tony Jesudasan uses only Reliance cellphone numbers. Sources say both the it Department and CBI wanted to tap Jesudasan's number but decided against it for obvious reasons. Singh had a friend in Vodafone's senior management who warned him of all his four numbers being monitored by the Delhi Police, thus giving him time to destroy incriminating evidence.

There is a twist in this tale. A majority of surveillance equipment was acquired to keep track of organised crime and terrorism. Intelligence agencies rue that phone tapping and interceptions are now yielding diminishing returns because terrorists have found new ways of staying ahead of them. Terrorists are increasingly using BlackBerry phones while their handlers are using the new generation Inmarsat-4 satellite phones, making their interception next to impossible, at least for now.

Though Inmarsat-4 phones can be monitored off the air, the conversation is available only in encrypted format. Voice and data can be effectively monitored only at the Inmarsat-4 switch in London and New York, where it is available in decrypted form. That is the reason why India still has to depend upon British or US intelligence agencies for information. Voice over Internet Telephony (voip)-based Skype and Google mail and chat are also extensively used by terrorists, small-time criminals and corporate houses. Free software can be downloaded on smart handsets and computers to encrypt calls and mails.

Commercially available software like Cellcrypt has been found to be most effective in securing conversations and messages. Compatible with all smartphones, Cellcrypt aids in personalised encryption of all communication. The only catch for completely secure communication is that handsets at both ends should have the software. If only one of the handsets has installed the software, the communication will be available in decrypted format at the other end.

The home ministry is now setting up what could be called a 'Big Brother server'. This move, done in sync with new laws on active phone interception, greatly enhances the Government's powers to snoop on individuals. At the heart of this plan is a Centralised phone and data monitoring centre costing Rs 800 crore. The Centre will improve coordination among the seven agencies authorised to tap phones and also with the states. "It will help centralise data collation and give the Central agencies actionable intelligence in more or less real time," says a home ministry official. It will also generate data about the number of phones being tapped countrywide.

The monitoring system will connect the small towns and cities of a state to its capital, and all the state capitals will be linked to a centralised monitoring centre in Delhi via fibre optic cables. If the IB wants to monitor a phone at Gonda in Uttar Pradesh, they can do so sitting in Delhi after sending necessary authorisations to the service provider. It will even make the process of tapping much smoother for the states since the capital city will be connected to the local switchboards. "It also increases the responsibility of the service provider since he is bound to deliver the traffic wherever asked," the official added. It will, for the first time, allow the Government to seamlessly monitor a suspect's cellphone across several networks and across the country. An intelligence official calls this the "nuclear weapon" of phone tapping software. "Implemented in its full form, it will give us the precise location of any individual within a cellphone network," he says.

This is why the Government plans to maintain the mandatory audit trail file, which will have electronic footprints of the number tapped-the agency given access for how long and if the conversation was recorded and if any copies were made. This protocol is followed worldwide and the audit file is crucial in the courts of countries where phone taps are

admissible as evidence. "In India, the protocol ensures no unauthorised copy is made and the system remains transparent," says an intelligence official, dealing with the project. Moreover, access to the audit file will only be through a valid password available with any of the Central agencies. Even service providers will not have access to it to rule out any tampering.

In an attempt to collate tapped data, the home ministry has asked the states for all records of phone and Internet interceptions. It also plans to supervise the working of the mandatory oversight committees on electronic surveillance in various states. At the Central level, the oversight committee is headed by the cabinet secretary and includes the law and telecom secretaries. With the home secretary approving most requests, the oversight committee is a mere formality. It rarely questions phone or Internet monitoring. Oversight committees on tapping in the states is tardily implemented. A few states don't even have these mandatory committees. The states that do have them rarely meet. Law and order being a state subject, the states are not bound to share the information.

Imagine this scenario. Terrorist A sends smses from Malad in Mumbai to terrorists B in Colaba and C in Bandra. The sms asks B and C to meet at Juhu beach, at 6 p.m. As B and C are moving, it becomes difficult to nab them by their cellphone location. The police alter the sms from A and send an sms saying "meet at Kalaghoda at 5 p.m." to B and "meet at Regal Cinema at 6 p.m." to C. B and C, believing that the sms was from A, respond accordingly. The police nab all three in a smooth operation.

Most anti-terror agencies can actually carry out such operations. Active off-air interception allows the police to virtually act as cellphone towers and thus modify or block smses and calls. The machine can be vehicle-mounted and can follow the target in urban areas where

conventional surveillance fails to track moving suspects. Security agencies say they have elaborate internal regulations to control the use of this technology. In Mumbai, for instance, the Crime Branch needs written authorisation from the police commissioner to use this machine. However, the temptation to misuse it for political espionage and personal gains is high. Conscious of its potential for misuse, the Uttar Pradesh ats has recently declined to acquire this tool. There is no guarantee that others will display such resolve.

TRUE COPY

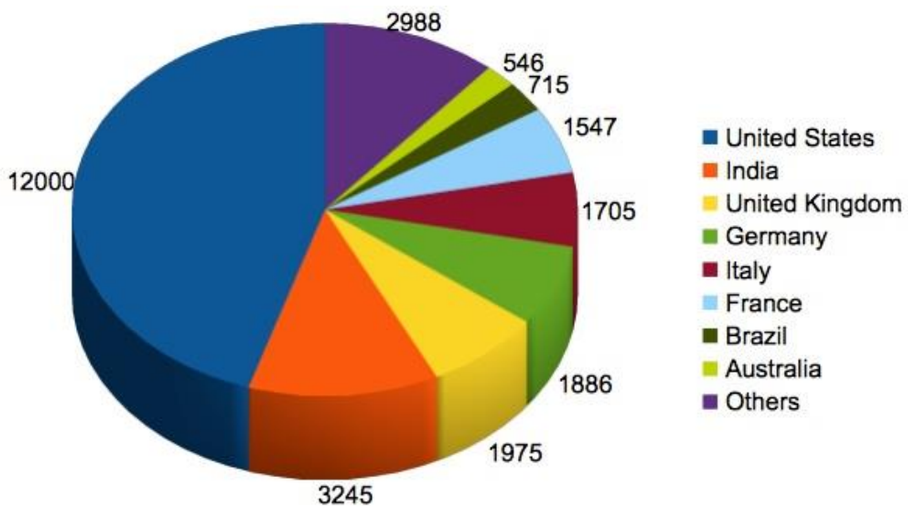
ANNEXURE P-7

sflc.in

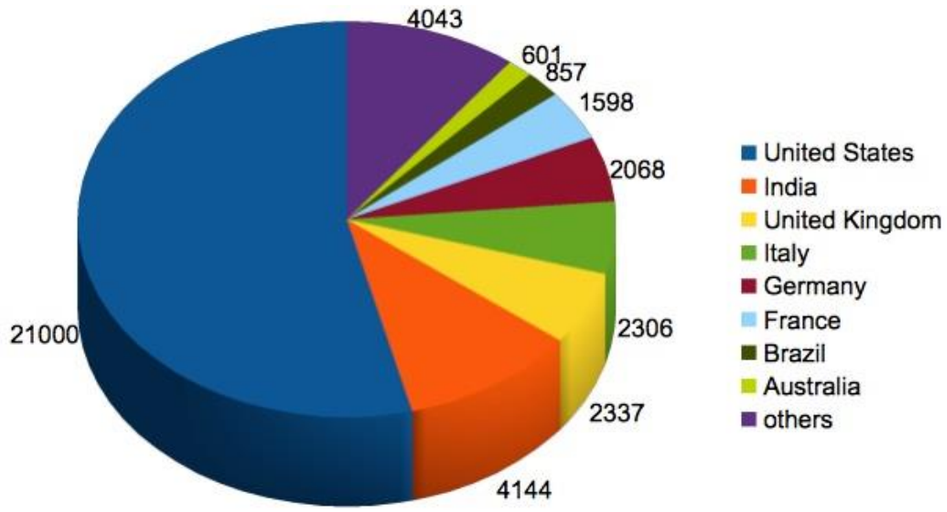
Surveillance - Is there a need for judicial oversight?

Wed, 09/25/2013 - 09:40
DIGITAL PRIVACY

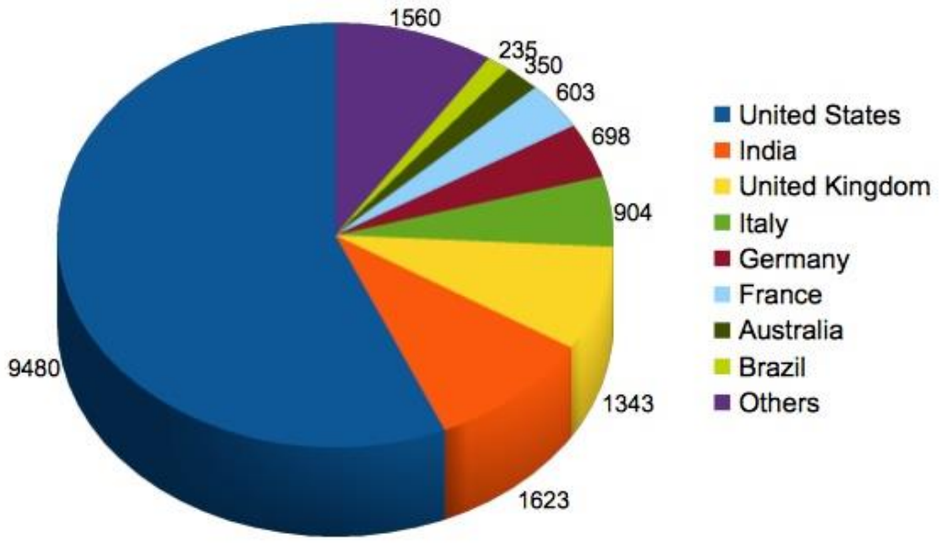
Recent reports released by Yahoo and Facebook on requests for user data sent by Governments paint a grim picture of surveillance. The transparency report released by Yahoo on September 6, 2013 shows that the Indian Government sent 1,490 requests asking information about 2,704 user accounts. On August 27, 2013, Facebook released its first Global Government Requests Report. The figures revealed in the report accord India, the dubious distinction of being the country with the highest number of user data requests after the United States. The United States Government submitted 11,000-12,000 requests to Facebook demanding information about 20,00-21,000 users while the Indian Government submitted 3,245 requests demanding information of 4,144 users during the period from January to June 2013.



Total No. of User Data requests by Governments



Total no. of user accounts requests by Governments



No. of requests complied by Facebook

The data earlier released by Google and Microsoft also portrays an alarming picture. The Indian Government sent 2431 user data requests to Google demanding information about 4106 users during July - December 2012. In the case of Microsoft, the Government sent 418 user data requests asking for information regarding 594 user accounts in 2012. Considering these numbers, the data sought by the Government from Indian online service providers ranging from Rediff.com to MouthShut.com could also be huge. However, no such information is available.

The biggest hurdle to get information related to requests made by the Government about electronic records is the provision in the

Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 which makes all this information confidential. Rule 25(4) of these Rules mandates that strict confidentiality has to be maintained in respect of direction for interception or monitoring. Although Section 22 of the Right to Information Act, 2005 overrides the provisions in any law which are inconsistent with the RTI Act, the Government often cites national security as the reason to prevent access to this information. Thus, all we have to gauge the quantum of electronic surveillance which is going on are the transparency reports released by these online service providers.

SFLC.IN had filed an application under the RTI Act to obtain information on tapping of telephones and monitoring of emails. The Ministry of Home Affairs in its reply dated August 6, 2013 has stated that on an average 7500 to 9000 orders for interception of telephones and 300 to 500 orders for interception of emails are issued by the Central Government every month. If you add to this the orders issued by the State Governments for telephone tapping and email monitoring, the numbers will be shocking.

These figures could only be the tip of the iceberg as the legal provisions make it fairly easy for law enforcement agencies to gather this data. In India, S.91 of the Code of Criminal Procedure, 1973 (CrPC) gives powers to any officer in charge of a police station to ask for production of any document for the purpose of investigation. This broad provision is often misused by law enforcement agencies to get information from Internet Intermediaries.

Moreover, sub-rule 7 of Rule 3 of the Information Technology (Intermediaries Guidelines) Rules, 2011 makes it even easier for any law enforcement agency to obtain information from an intermediary.

In addition to this, the Controller of Certifying Authorities(CCA) also has the power to request information from providers. Earlier, the CCA in reply to an application that we had filed under the RTI Act informed us that the CCA has received 103 requests for investigation from all agencies of the Government of India and State governments in the last three years and that the CCA has issued notices to Intermediaries in 73 instances. The CCA had in fact fined Yahoo for not complying with its order to provide user information. The Writ petition filed by Yahoo before the High Court of Delhi challenging this order and Rule 7(3) of the Intermediaries Guidelines Rules is pending.

Such broad provisions in the law, combined with the absence of a legislation which restricts such requests, has resulted in the Government and its agencies sending huge number of user data requests to service providers. These requests are made by agencies ranging from the Home Ministry to the local police stations. The huge numbers show that there clearly is a need for proper safeguards to be built into the system to protect the right to privacy of citizens. The sheer number of telephone tapping orders issued per month shows that the current mechanism consisting of top level officials for reviewing tapping orders, which is supposed to be a safeguard has been reduced to a mere formality.

There is an urgent need to evolve a proper legal framework to protect privacy of citizens when Government agencies request user information and monitor telephonic and electronic communication. The Supreme Court in the PUCL case had framed various guidelines to be observed while issuing orders to tap telephones. The review mechanism by which the tapping orders are reviewed by a team consisting of the Cabinet Secretary, Secretary in the Ministry of Law Affairs and Secretary of the Department of Telecommunications in the Centre and a similar mechanism in the

state has in effect resulted in a system where the powers for issuing orders, execution and review are with the executive. The current legal framework as per the Telegraph Act or the Information Technology Act do not provide for a judicial oversight. In fact, the Supreme Court held in the PUCL case that that in the absence of any provision in the statute, it is not possible to provide for prior judicial scrutiny as a procedural safeguard. In view of the current surveillance rich environment cloaked in secrecy, it is time to start discussing whether judicial interference is required to balance privacy of citizens with compelling interests of the state.

TRUE COPY

ANNEXURE P-8

RTI Matter
Speed Post

No. II20034/35/2011-IS.II
Government of India
Ministry of Home Affairs
(IS.I Division/IS.II Desk)

New Delhi; dated the 25th May, 2011

To

Shri Paras Nath Singh,

Sub: Application of Shri Paras Nath Singh seeking information under Right to Information Act, 2005.

Sir,

Please refer to this Ministry's Order dated 2.5.2011 passed by the Appellate Authority, Shri Dharmendra Sharma, Joint Secretary (IS.I), Ministry of Home Affairs, against your appeal dated 8.4.2011 wherein you were directed to approach CPIO once again to obtain information with regard to para 1.

2. In connection with para 1 of your application dated 24.2.2011, it is stated that on an average, between 7500 to 9000 orders for interception of telephones are issued by the Central Government per month.

Yours faithfully.

S/d.
(V. Vumlunmang) Director (Internal Security-I)

Copy to Shri S. Padmanabha, Under Secretary & Dy. Registrar, CIC, 2' Floor, August Kranti Bhavan, Bhikaji Cama Plaice, New Delhi — w.r.t. appeal dated 16.5.2011 filed in the CIC by Shri Paras Nath Singh,

TRUE COPY

ANNEXURE P-9

GOVERNMENT OF INDIA

MINISTRY OF HOME AFFAIRS

LOK SABHA
STARRED QUESTION NO: 294

ANSWERED ON: 11.02.2014

PHONE TAPPING

M. K. RAGHAVAN

Will the Minister of HOME AFFAIRS be pleased to state:-

(a) whether there are reports of illegal telephone tapping and collection of call details both by the Government and private agencies;

(b) if so, the details thereof and the action taken in this matter by the Government;

(c) whether there are any guidelines/legal provisions under which telephonic conversations can be intercepted and call details collected by various agencies;

(d) if so, the details thereof indicating the names of the agencies authorised in this regard; and

(e) the details of the steps taken/being taken by the Government to prevent the misuse of powers for intercepting conversations, safeguarding the audio recording/transcripts of such intercepted conversations and preventing leakage of the same?

ANSWER

MINISTER OF STATE IN THE MINISTRY OF HOME AFFAIRS (SHRI R.P.N SINGH)

(a) to (e) A Statement is laid on the Table of the House.

STATEMENT IN REPLY TO PARTS (a) to (e) OF THE LOK SABHA STARRED QUESTION NO.294 FOR 11TH FEBEUARY,2014.

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

(c)&(d) Interception of communication by authorized Law Enforcement Agencies (LEAs) is carried out in accordance with Section 5(2) of the Indian Telegraph Act, 1885 read with Rule 419A of Indian Telegraph (Amendment) Rules, 2007. Following is the list of authorised Law Enforcement Agencies for Lawful Interception:

Central Agencies

(i) Intelligence Bureau,
(ii) Narcotics Control Bureau,
(iii) Directorate of Enforcement,
(iv) Central Board of Direct Taxes,
(v) Directorate of Revenue Intelligence,
(vi) Central Bureau of Investigation,
(vii) National Investigation Agency,
(viii) Research & Analysis Wing (R&AW),
(ix) Directorate of Signal Intelligence, Ministry of Defence- for Jammu & Kashmir, North East & Assam Service Areas only.

State Agencies

Director General of Police, of concerned state/Commissioner of Police, Delhi for Delhi Metro City Service Area only.

Call data records (CDRs) can be sought by following the statutory provisions contained in Section 92 of the Code of Criminal Procedure, 1973 or Section 5(2) of the Indian Telegraph Act, 1885 read with Rule 419 A of Indian Telegraph (Amendment) Rules, 2007.

(e) Standard Operating Procedures for Interception, Handling, Use, Sharing, Copying, Storage and Destruction of records have been issued by the Ministry of Home Affairs to the Central Law Enforcement Agencies. The Department of Telecom has issued Standard Operating Procedures for Lawful Interception to the Telecom service providers.

The orders of the competent authority authorising Lawful Interception are reviewed by a Review Committees constituted under Rule 419 A of the Indian Telegraph (Amendment) Rule, 2007.

TRUE COPY

ANNEXURE P-10

GOVERNMENT OF INDIA

MINISTRY OF HOME AFFAIRS

RAJYA SABHA
QUESTION NO 3107

ANSWERED ON 29.03.2017

Cyber filtering of extremist antinational contents

3107 Shri B.K. Hariprasad

Will the Minister of HOME AFFAIRS be pleased to state :-

(a) whether the Ministry is planning to create any mechanism to ensure cyber filtering of the extremist/anti-national contents present in the cyber world;
(b) if so, the details thereof;
(c) if not, the reasons therefor; and
(d) the details of steps taken in this regard?

ANSWER

MINISTER OF STATE IN THE MINISTRY OF HOME AFFAIRS
(SHRI HANSRAJ GANGARAM AHIR)

(a) to (d): The security and intelligence agencies monitor the cyber space and whenever they notice any objectionable online content relating to sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence, necessary action is taken for the blocking of such online content as per the provisions of Section 69A of the Information Technology Act, 2000.

TRUE COPY

ANNEXURE P-11

RTI Request Details

RTI Request Registration number	MHOME/R/2018/53841
Public Authority	Ministry of Home Affairs

Personal Details of RTI Applicant:-

Name	Apar Gupta
Gender	Male
Address	E-215, Third Floor, East of Kailash , New Delhi
Pincode	110065
Country	India
State	Delhi
Status	Urban
Educational Status	Literate
Phone Number	Details not provided
Mobile Number	+91-9990000256
Email-ID	policy[at]internetfreedom[dot]in

Request Details :-

Citizenship	Indian
Is the Requester Below Poverty Line ?	No

(Description of Information sought (upto 500 characters)

Description of Information Sought

The following request pertains to orders or directions issued by the Competent Authority under Section 69 of the Information Technology Act, 2000 and IT (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009:

1. Provide the total number of orders passed by the Competent Authority in exercise of powers under Section 69 of the IT Act read with Rule 3, between 01.01.2016 and 27.12.2018.

2. Provide the total number of requests received under Section 69 and Rules thereunder from various agencies between 01.01.2016 and 27.12.2018

3. Provide the total number of requests received under Section 69 and Rules thereunder from various agencies that were rejected or not authorized between 01.01.2016 and 27.12.2018

4. Provide the total number of approval requests received during 01.01.2016 to 27.12.2018 (as per Proviso (ii) to Rule 3), to validate interception, monitoring or decryption citing cases of emergency viz., (a) remote areas and (b) operational reasons. In addition, provide a breakup of requests under both the categories

5. Provide the total number of approval requests received during 01.01.2016 to 27.12.2018 (as per Proviso (ii) to Rule 3) that were not approved or revoked by the Competent Authority, between 01.01.2016 and 27.12.2018

Concerned CPIO Nodal Officer

Supporting document
(only pdf upto 1 MB) Supporting document not provided

RTI Request Details

RTI Request Registration number	MHOME/R/2018/53842
Public Authority	Ministry of Home Affairs

Personal Details of RTI Applicant:-

Name	Apar Gupta
Gender	Male
Address	E-215, Third Floor, East of Kailash , New Delhi
Pincode	110065
Country	India
State	Delhi
Status	Urban
Educational Status	Literate
Phone Number	Details not provided
Mobile Number	+91-9990000256
Email-ID	policy[at]internetfreedom[dot]in

Request Details :-

Citizenship	Indian
Is the Requester Below Poverty Line ?	No

(Description of Information sought (upto 500 characters)

Description of Information Sought

The following request pertains to orders or directions issued by the Competent Authority under Section 69 of the Information Technology Act, 2000 and IT (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009:

1. Provide the total number of orders or directions issued by the

Competent Authority for prevention of any offence affecting the sovereignty or integrity, defense, or security of the State, between 01.01.2016 and 27.12.2018.

2. Provide the total number of orders or directions issued by the Competent Authority for investigation of any offence, between 01.01.2016 and 27.12.2018.

Concerned CPIO Nodal Officer

Supporting document
(only pdf upto 1 MB) Supporting document not provided

RTI Request Details

RTI Request Registration number	MHOME/R/2018/53844
Public Authority	Ministry of Home Affairs

Personal Details of RTI Applicant:-

Name	Apar Gupta
Gender	Male
Address	E-215, Third Floor, East of Kailash , New Delhi
Pincode	110065
Country	India
State	Delhi
Status	Urban
Educational Status	Literate
Phone Number	Details not provided
Mobile Number	+91-9990000256
Email-ID	policy[at]internetfreedom[dot]in

Request Details :-

Citizenship	Indian
Is the Requester Below Poverty Line ?	No

(Description of Information sought (upto 500 characters)

Description of Information Sought

The following request pertains to orders or directions issued by the Competent Authority under Section 69 of the Information Technology Act, 2000 and IT (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009:

Please provide the names of agencies along with number of orders or

directions issued to them by the Competent Authority for interception, monitoring, or decryption between 01.01.2016 and 27.12.2018.

Concerned CPIO Nodal Officer

Supporting document
(only pdf upto 1 MB) Supporting document not provided

RTI Request Details

RTI Request Registration number	MHOME/R/2018/53845
Public Authority	Ministry of Home Affairs

Personal Details of RTI Applicant:-

Name	Apar Gupta
Gender	Male
Address	E-215, Third Floor, East of Kailash , New Delhi
Pincode	110065
Country	India
State	Delhi
Status	Urban
Educational Status	Literate
Phone Number	Details not provided
Mobile Number	+91-9990000256
Email-ID	policy[at]internetfreedom[dot]in

Request Details :-

Citizenship	Indian
Is the Requester Below Poverty Line ?	No

(Description of Information sought (upto 500 characters)

Description of Information Sought

The following request pertains to orders or directions issued by the Competent Authority under Section 69 of the Information Technology Act, 2000 and IT (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009:

1. Provide the total number of orders or directions issued by the Competent Authority to authorize monitoring, interception, or

decryption for a continued period more than 15 days.

2. Provide the total number of orders or directions renewed by the Competent Authority for a period exceeding 60 days, between 01.01.2016 and 27.12.2018.

3. Provide the total number of orders or directions revoked or withdrawn or rescinded prior to the sunset period or the 60-day period prescribed under Rule 11.

Concerned CPIO Nodal Officer

Supporting document
(only pdf upto 1 MB) Supporting document not provided

RTI Request Details

RTI Request Registration number	MHOME/R/2018/53846
Public Authority	Ministry of Home Affairs

Personal Details of RTI Applicant:-

Name	Apar Gupta
Gender	Male
Address	E-215, Third Floor, East of Kailash , New Delhi
Pincode	110065
Country	India
State	Delhi
Status	Urban
Educational Status	Literate
Phone Number	Details not provided
Mobile Number	+91-9990000256
Email-ID	policy[at]internetfreedom[dot]in

Request Details :-

Citizenship	Indian
Is the Requester Below Poverty Line ?	No

(Description of Information sought (upto 500 characters)

Description of Information Sought

The following request pertains to orders or directions issued by the Competent Authority under Section 69 of the Information Technology Act, 2000 and IT (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009:

1. Provide the total number of directions issued under Section 69

and Rules thereunder for interception, monitoring, or decryption in relation to any specific information stipulated under Rule 9.

Concerned CPIO Nodal Officer

Supporting document
(only pdf upto 1 MB) Supporting document not provided

RTI Request Details

RTI Request Registration number	MHOME/R/2018/53847
Public Authority	Ministry of Home Affairs

Personal Details of RTI Applicant:-

Name	Apar Gupta
Gender	Male
Address	E-215, Third Floor, East of Kailash , New Delhi
Pincode	110065
Country	India
State	Delhi
Status	Urban
Educational Status	Literate
Phone Number	Details not provided
Mobile Number	+91-9990000256
Email-ID	policy[at]internetfreedom[dot]in

Request Details :-

Citizenship Indian

Is the Requester Below Poverty Line ? No

(Description of Information sought (upto 500 characters)

Description of Information Sought

The following request pertains to orders or directions issued by the Competent Authority under Section 69 of the Information Technology Act, 2000 and IT (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009:

1. Provide the total number of orders or directions issued by the Competent Authority, other than the Secretary (MHA) i.e., Joint

Secretaries, between 01.01.2016 and 27.12.2018.

2. Provide the date, time, and duration of meetings conducted by the Review Committee during 01.01.2016 and 27.12.2018 to review orders or directions issued pursuant to Section 69.

Concerned CPIO Nodal Officer

Supporting document
(only pdf upto 1 MB) Supporting document not provided

TRUE COPY

IN THE SUPREME COURT OF INDIA

CIVIL ORIGINAL JURISDICTION

I. A. NO. OF 2019

IN

WRIT PETITION (CIVIL) NO. OF 2019

IN THE MATTER OF:-

Internet Freedom Foundation
& Another … PETITIONERS

VERSUS

Union of India & Others … RESPONDENTS

AN APPLICATION FOR *EX-PARTE* INTERIM STAY / DIRECTIONS

To,

The Hon'ble Chief Justice of India
and His Companion Judges of
the Hon'ble Supreme Court of India

The Humble Petition of the
Petitioners above named

1. The accompanying Petition under Article 32 of the Constitution of India, filed in public interest, seeks to challenge the constitutional validity of Section 69 of the Information Technology Act, 2000 ["**IT Act**"] and The Information Technology (Procedure for Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 ["**2009 IT Rules**"] enacted pursuant to Section 69(2) read with Section 87(2)(y) of the Act, for being violative of Articles 14, 19(1)(a) and 21 of the Constitution. Consequently, the Petitioners seek a writ of *certiorari* or any other appropriate writ, order, or

direction to quash the Notification dated 20.12.2018 (bearing No. 14/07/2011-T) ["**Impugned Notification**"], wherein ten (10) Security and Intelligence Agencies ["**Authorised Agencies**"] of the Central Government have been authorised to intercept, monitor, and decrypt [collectively as "**Electronic Surveillance**"] any information generated, transmitted, received, or stored in any computer resource.

2. The Petitioners are constrained to prefer the instant application, to seek an *ex-parte* interim stay of the operation of Impugned Provisions, i.e. Section 69 of the IT Act and the 2009 IT Rules, for being violative of Articles 14, 19, 20 and 21 of the Constitution of India. At the outset, the Petitioners state that the aforesaid provisions adversely impact the right to privacy and fail the test of proportionality, the substantive contents of which have been fleshed out in **K. S. Puttaswamy v. Union of India** (2017) 10 SCC 1 ["**Puttaswamy (*Privacy*)**"] and **K. S. Puttaswamy v. Union of India** (2018) 12 SCALE 1 ["**Puttaswamy (*Aadhaar*)**"]. In addition, the Petitioners also seeks a stay on the impugned Notification dated 20.12.2018 issued by Respondent No. 2, being illegal and *ultra vires* Section 69(1) of the IT Act.

3. The Impugned Notification, the first of its kind issued under Section 69(1) of the IT Act and Rule 4 of the 2009 IT Rules, has essentially activated the unconstitutional surveillance mechanism erected by the Act and Rules, necessitating urgent intervention by this Hon'ble Court, especially since the institutional structure created provides for no judicial oversight which, would be a minimum requirement for the provisions in question to pass muster from a constitutional standpoint.

4. Further, the security and intelligence agencies that have been notified and authorised under the impugned notification to carry

out the interception, monitoring and decryption activities, particularly the Intelligence Bureau, Central Bureau of Investigation, and the Cabinet Secretariat (Research & Analysis Wing) lack a statutory basis, and are therefore hit by the **Puttaswamy** (*Privacy*) and **Puttaswamy** (*Aadhaar*) standard. It is now well settled that any infringement on the right to privacy has to be authorised by law. However, although the surveillance requires are sanctioned under the IT Act, the agencies that have been notified to carry them out are not authorised by law. Thus, to the extent that the impugned Notification authorises these agencies, it is further unconstitutional.

5. Be that as it may, the information available in public domain reveal that the safeguards suggested by this Hon'ble Court in **PUCL Wiretapping** (*supra*) have not been effectively implemented by the Respondents and reveal a malice of inadequate institutional capacity and credible oversight on use of surveillance regulations. For example:

(a) At any given point of time, the Authorised Agencies maintain surveillance on a large number of telephones and electronic devices. According to a news report published in India Today on 20.12.2010, more than 6,000 telephones were under watch in New Delhi alone. The list included bureaucrats, military officials, corporates, journalist and NGOs. [*Ref.* **ANNEXURE P-6 (Page Nos. 111 to 119)**]

(b) The Competent Authority receives and grants authorisation to a large number of surveillance requests. In response to an RTI request filed by "SLFC.in" in 2013, the Respondent No. 2 has stated that "on an average 7500 to 9000 orders for interception of telephones and 300 to 500 orders for interception of emails are issued by the Central Government every month." Given the large number of

requests, it is highly improbable that the Competent Authority has adequate time and opportunity to make an effective assessment on alternative means of acquiring information. [*Ref.* **ANNEXURE P-7 (Page Nos. 120 to 124)**]

(c) As noted by the Justice Srikrishna Committee (at Pg. 125), the Review Committee usually convenes once every two months, and has the "unrealistic task" of reviewing more than 15,000-18,000 surveillance orders in every meeting.

6. The above statistics raise serious alarm on the institutional capacity of the Competent Authority and the Review Committees to handle, authorise, and review surveillance requests. Egregiously, the Central Government has admitted on the floor of Parliament that the "Incidents of physical/electronic surveillance in the States of Gujarat and Himachal Pradesh, and the National Capital Territory of Delhi, allegedly without authorization have been reported. Union Cabinet has approved a proposal to set up a Commission of Inquiry under Commission of Inquiry Act, 1952 to look into these incidents."

7. Thus, the Petitioners are constrained to file the present application since there is little or no possibility of individuals detecting and complaining of legal injury, given the covert nature of electronic surveillance, and it is thus imperative for this Hon'ble Court to stay the impugned provisions and impugned Notification, while adjudging the constitutionality of the surveillance system, whose very existence, in the absence of oversight, impacts the fundamental rights of citizens.

8. Further, in the absence of parliamentary or judicial oversight, the power to intercept, decrypt and monitor gives the executive government the power to influence the subject of surveillance

and all classes of persons, without any checks outside the executive wing of government.

9. The very act of surveillance – taken on its own – infringes fundamental rights under Articles 19(1)(a) and 21. While the "harm" that surveillance causes cannot be quantified in a physical or tangible form, this Hon'ble Court has never insisted upon a showing of physical injury as a threshold requirement to demonstrate the violation of a fundamental right. The Petitioners respectfully submit that the very existence of a surveillance system impacts the right to privacy and chills the exercise of liberties under Articles 19 and 21.

10. The Petitioners submit that, in light of the law laid down in **Puttaswamy** (*Privacy*) and **Puttaswamy** (*Aadhaar*), the lack of any oversight, in itself, warrants a finding that the Impugned Provisions and the Impugned Notification are unconstitutional for the following reasons:-

i. Apart from disturbing the horizontal separation of powers, as mentioned hereinabove, the concentration of disproportionate power in the hands of the executive under the Impugned Provisions and Impugned Notification would violate the requirement of having adequate procedural safeguards, as mandated in **Puttaswamy** (*Privacy*). Therefore, oversight by another branch of government would be the minimum requirement for surveillance provisions to pass muster.

ii. Specifically, based on the rulings in **Puttaswamy** (*Privacy*) and **Puttaswamy** (*Aadhaar*), judicial oversight would be the minimum requirement for this system to pass constitutional muster, as the judiciary alone is competent to decide whether specific instances of surveillance are proportionate, especially to decide whether less onerous

alternatives are available and in balancing the importance of the government objective with the rights of the individual / individuals impacted. It is obvious that a Court, alone, is competent to decide the constitutionality of individual instances of surveillance and test it on the proportionality standard. Nothing in the Court rulings in **Puttaswamy** (*Privacy*) and **Puttaswamy** (*Aadhaar*) suggests that a finding on proportionality can be returned by an executive authority.

iii. However, the requirement of judicial oversight goes beyond the issue of institutional competence. It is also an minimum requirement in order to satisfy the requirement of "due process". By design, surveillance - which operates in secret - curtails the operation of Articles 32 and 226 of the Constitution, as a person who suspects that she is under surveillance, in many cases will have no way of proving it, and cannot therefore establish a breach in accordance with Articles 32 and 226, until that information is revealed. The effective exclusion of Articles 32 and 226 therefore entails that, for all practical purposes, the decision of the Executive on whether fundamental rights have been validly and reasonably infringed, is final. It is respectfully submitted that this violates the requirements of fairness and due process under Article 21, as well as the broader requirements of natural justice. This denial of judicial scrutiny amounts to an effective denial of remedies under Article 21 of the Constitution. In the absence of a judicial determination that surveillance meets the proportionality standards under Article 21, the lack of ability to approach the courts effectively entails the denial of the right itself.

iv. Additionally, authorizing incursions into the private domain in the course of "investigation" is, traditionally,

within the exclusive domain of the judiciary alone (akin to the judiciary's power to issue warrants for search and seizure of premises), and the fact that Section 69 of the IT Act can be deployed in the investigation of criminal offences without any judicial oversight buttresses the Petitioners' case that the Impugned Provisions and the Impugned Notification run contrary to the horizontal separation of powers established under the Constitution of India.

11. In the above premises, it is submitted that the Impugned provisions, namely Section 69 of the IT Act and the 2009 IT Rules, as well as the Impugned Notification dated 20.12.2018 issued by Respondent No. 2 is liable to be quashed and is also violative of Articles 14, 19 and 21 of the Constitution. Thus, the balance of convenience is in favour of the Petitioners.

12. While the main prayers in this application seek stay of the operation of Section 69 of the IT Act and the 2009 IT Rules, it is humbly prayed, in the alternative, that since surveillance (as per the law laid down by this Hon'ble Court) directly impacts the right to privacy, it is imperative that (if stay is not granted) that every individual order for interception, monitoring, decryption etc. passed by the competent authority under Section 69 of the IT Act read with the 2009 IT Rules be placed before this Hon'ble Court, and that no agency ought to carry out interception, monitoring and decryption unless this Hon'ble Court confirms the competent authority's order in each individual case. Such scrutiny would be necessary to analyze whether there is a rational nexus between the decryption order and the objectives set out in Section 69(1); to decide whether less onerous alternatives are available; and, to balance the importance of the government objective with the rights of the individual / individuals impacted. If such orders are not scrutinized by this

Hon'ble Court during the pendency of the present petition, unconstitutional surveillance orders would, essentially, escape any judicial scrutiny whatsoever. Furthermore, scrutiny by this Court would, in the interregnum, mitigate the chilling effect of such a surveillance infrastructure, as a constitutional court would be balancing individual rights against surveillance orders issued by the executive government.

13. The function of scrutiny may, in the alternative, be vested with a in a Committee, constituted by this Hon'ble Court, comprising of sitting Judges of this Hon'ble Court and/or sitting Judges of the High Courts, which would scrutinize/review the directions/orders passed by the Competent Authority under Section 69 of the Information Technology Act, 2000 read with the 2009 IT Rules.

14. It is humbly submitted that the present application is *bona fide* it would therefore be in the interest of justice if this Hon'ble Court grants interim reliefs as prayed for. No prejudice will be caused to the Respondents, if the instant application is allowed.

PRAYER

In the premises, it is most respectfully prayed that this Hon'ble Court may be pleased to –

A. Stay the effect and operation of Section 69 of the Information Technology Act, 2000;

B. Stay the effect and operation of Information Technology (Procedure for Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009;

C. Stay the effect and operation of Notification dated 20.12.2018 (bearing No. 14/07/2011-T) issued by Respondent No. 2, and thereby restrain the Respondents/their authorities/agents and the agencies authorised under Impugned Notification dated

20.12.2018 from enforcing the Notification during the pendency of the Petition;

D. Pass an *ad* interim *ex parte* order of stay in terms of Prayers (A) to (C) above and confirm the same after notice to Respondents;

E. In the alternative to Prayers (A) to (C), direct Respondent No. 2 to place every order for interception, monitoring, or decryption issued under Section 69 of the IT Act read with the 2009 IT Rules before this Hon'ble Court, and restrain all agencies from carrying out interception, monitoring and decryption without leave from this Hon'ble Court;

F. In the alternative to Prayer (E), pass appropriate Orders constituting a Committee comprising of sitting Judges of this Hon'ble Court and/or sitting Judges of the High Courts to scrutinize/review the directions/orders passed by the Competent Authority under Section 69 of the Information Technology Act, 2000 read with the 2009 IT Rules.

G. Pass such other and further orders as this Hon'ble Court may deem fit in the instant facts and circumstances.

FILED BY:

DRAWN ON : 03.01.2019
FILED ON : 08.01.2019

ADVOCATE FOR THE PETITIONERS
PRATEEK CHADDHA