India's Surveillance State

sflc.in

WORLD WIDE WEB FOUNDATION

Communications Surveillance in India

Table of contents

List of statutes

Indian Telegraph Act, 1885

Indian Telegraph Rules, 1951

Information Technology Act, 2000

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

Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009

Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

Information Technology (Intermediaries Guidelines) Rules, 2011

Information Technology (Guidelines for Cyber Cafe) Rules, 2011

Code of Criminal Procedure, 1973

List of cases

List of abbreviations

C-DOT	Centre for Development of Telematics
CAIR	Centre for Artificial Intelligence and Robotics
CCA	Controller of Certifying Authorities
CCPR	Centre for Civil and Political Rights
CBDT	Central Board of Direct Taxes
CBI	Central Bureau of Investigation
CDR	Call Data Record
CMS	Centralized Monitoring System
CrPC	Criminal Procedure Code
DIA	Defense Intelligence Agency
DOT	Department of Telecommunications
DRDO	Defense Research and Development Organization
DRI	Directorate of Revenue Intelligence
ED	Enforcement Directorate
GB	Giga-byte
GoI	Government of India
GPS	Global Positioning System
HCHR	High Commissioner on Human Rights
HRC	Human Rights Commission
IB	Intelligence Bureau
ICCPR	International Covenant on Civil and Political Rights
IP	Internet Protocol
IPDR	Internet Protocol Data Record
IPTV	Internet Protocol Television
ISF	Information Store and Forward
ISL	Internet Service License
ISP	Internet Service Provider
IT Act	Information Technology Act

TRAI	Telecom Regulatory Authority of India
TSP	Telecom Service Provider
UASL	Unified Access Service License
UDHR	Universal Declaration on Human Rights
US	United States
UL	Unified License
UN	United Nations

1. Introduction

In June 2013, the world was treated to a rude awakening by a hitherto unknown Edward Snowden, when he made public thousands of classified documents that belonged to the United States' National Security Agency (NSA). Described as one of the most significant leaks in US history, the disclosed documents revealed that the US Government had been discreetly collecting unprecedented quantities of surveillance data on everyone from its own citizens to foreign Governments, ostensibly as part of its global war against terror.

While most of the rest of the world was foreseeably outraged by the contents of Snowden's revelations, the then Indian Government's response to the matter was tepid at best, and the whole affair was shrugged off as a routine occurrence in international diplomacy. This stand was especially surprising since India, who has always boasted friendly ties with the US, was reportedly fifth in the overall list of countries spied on by the NSA programs. Why then was India rushing to the US' defense, with the then Minister for External Affairs going so far as to say that the US surveillance programs are "not actually snooping"?

On closer inspection, one quickly begins to realize that the Government of India's (GoI) tolerance of US surveillance might have been brought on by more than a mere desire to keep Indo-US relations from going sour. In line with the age-old adage against throwing stones in a glass house, the Government's remarkable restraint might have stemmed – at least in part – from the fact that it was busy with some "snooping" of its own. While we note with great satisfaction the earnest words of the current Minister of External Affairs, Ms. Sushma Swaraj on issues of US surveillance and hope the matter will get the attention it deserves, the need to understand India's domestic surveillance practices is not obliterated.

> Multiple Indian legislations ... contain explicit provisions that allow Central and State Governments to intercept and monitor the nation's communication networks on several grounds.

Multiple Indian legislations, including the Indian Telegraph Act and Rules, Information Technology Act and Rules and the Code of Criminal Procedure, contain explicit provisions that allow Central and State Governments to intercept and monitor the nation's communication networks on several grounds. These grounds are often broadly worded, with generous helpings of terms such as 'security of the state' and 'public safety' that are never defined with any manner of precision. This effectively grants the Government unsubstantiated access to India's telephone and Internet networks to retrieve their contents at will. Similarly, license agreements entered into between Indian communications service providers and the Department of Telecommunications contain clauses that mandate *inter alia*, the installation of unspecified surveillance equipment into communication networks as and when required by the Government and its

agents. All service providers operating within the country at any given point of time are therefore bound to ensure that their networks are open to Government surveillance.

Under the authority of the aforementioned provisions of law, a number of Lawful Interception and Monitoring (LIM) systems have been installed into India's telephone and Internet networks. These bare in real-time our phone calls, texts, e-mails and general Internet activity to Government surveillance. 'LIM systems' being a generic term that alludes to any surveillance system sanctioned by law, the true nature and extent of capabilities of the specific systems employed by the Indian Government remain matters of intelligent speculation. Aside from these pre-existing LIM systems, a slew of additional surveillance systems designed to significantly enhance the Government's existing capabilities are also in the pipeline in varying stages of deployment. This includes as of current knowledge, the Central Monitoring System (CMS), Network Traffic Analysis (NETRA), and National Intelligence Grid (NATGRID) – all of which will be examined in detail in the course of this report.

An application filed by SFLC.in under the Right to Information Act revealed that on an average, around *7500 – 9000* telephone-interception orders are issued by the Central Government alone *each month*. Extrapolating this number to include all interception orders issued by the Central and State Governments combined, it becomes clear that Indian citizens are routinely and discreetly subjected to Government surveillance on a truly staggering scale.

In this report, SFLC.in delves into the unchartered wilderness that is India's surveillance landscape in a pragmatically pessimistic bid to demystify our surveillance practices. In order to keep the scope of research within the realm of feasibility, this report will restrict itself to Indian *communications* surveillance i.e. surveillance of telephones and the Internet. In this regard, we will take an in-depth look at various aspects of India's surveillance machinery, including enabling provisions of law, service provider obligations, and known surveillance mechanisms. We will offer recommendations aimed at bettering what our readers will hopefully see is a lamentable state of affairs.

We express our sincere gratitude to the Web We Want campaign, without whose invaluable contributions this report would not have been possible.

2. Enabling Statutes

It is only fitting that any study of India's communications surveillance landscape commence with the various provisions of law whence the Government derives its broad powers. Accordingly, we now turn to statutes that enable surveillance of the two most widely subscribed modes of communication and information exchange in India *viz.* telephones and the Internet.

2.1 Telephones

When it comes to surveillance of telephone networks, the **Indian Telegraph Act, 1885** serves as the primary enabling statute. The definition of the term "*telegraph*" as provided under **Section 3(1AA)** of the Act goes above and beyond its linguistic connotations, and includes "*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 electro-magnetic emissions, radio waves or Hertzian waves, galvanic, electric or magnetic means*". It is this broad and future-proof definition that brings virtually any communication device – including telephones – within the Act's purview.

> The occurrence of a public emergency or the interest of public safety are therefore pre-requisites for the invocation of Section 5(2)

Going forward, **Section 5(2)** of the Telegraph Act provides for telephone tapping by the Government. It reads:

"*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.*"

The occurrence of a public emergency or the interest of public safety are therefore pre-requisites for the invocation of Section 5(2). In the absence of either, the Government is disallowed from intercepting communications made over telephones. While the terms 'public emergency' and 'public safety' are not defined under the Act itself, they were interpreted by the Supreme Court of India in the matter of *People's Union for Civil Liberties v. Union of India*[1] to mean "*the prevalence of a sudden condition or state of affairs affecting the people at large calling for immediate action*", and "*the state or condition of freedom from danger or risk for the people at large*" respectively.

To recap, if either of the above conditions

1 AIR 1997 SC 568

are met, Central/State Governments or any of their authorized officers may direct that communications made over telephones be intercepted, if such interception is considered necessary or expedient in the interest of:

- Sovereignty/integrity of India
- Security of the State
- Friendly relations with foreign States
- Public order
- Prevention of incitement to the commission of any offence

None of the above five expressions have been defined under the Telegraph Act, which means they are open to interpretation by the concerned authority that sanctions interception.

With the *substantive* law regarding telephone tapping laid out by Section 5(2), the *procedural* law regarding the same is found under **Rule 419A** of the **Indian Telegraph Rules, 1951**. It is important to note that Rule 419A was not part of the Telegraph Rules when they were originally notified in 1951. It was introduced by way of an amendment in 2007, which was necessitated by the Supreme Court's condemnation in PUCL[2] of the lack of procedure governing telephone tapping. Due to this absence of procedure, the Supreme Court in PUCL had also enumerated certain guidelines to be followed while intercepting communications under Section 5(2). These guidelines served as a place-holder up until 2007, when Rule 419A was officially added to the Telegraph Rules, replacing the Court-issued guidelines.

As the procedure laid down by Rule 419A is lengthy and complicated to say the least, it will be examined in two phases – (1) procurement and review of lawful order, and (2) interception process.

2 Supra. 1

2.1.1 Procurement and review of lawful order under Rule 419A

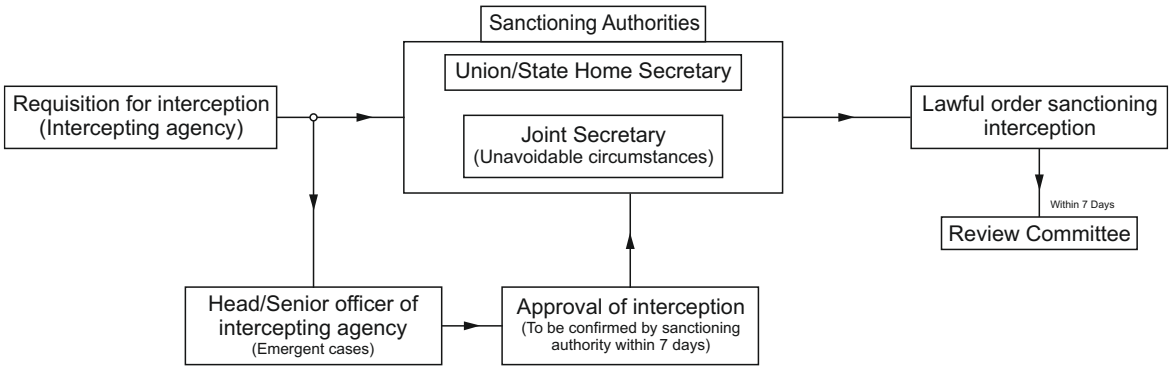

Fig. 1 – Procurement and review of lawful order

According to Rule 419A, a direction for interception under Section 5(2) [hereinafter referred to as the 'lawful order'] may normally be issued only by the Union Home Secretary at the Centre, or a State Home Secretary at the States. However, in *unavoidable circumstances*, a lawful order may be issued by an officer not below the rank of a Joint Secretary to the Government of India, who has been authorized by the Union/State Home Secretary to this effect.

> Rule 419A also states that a lawful order may be issued only once all other reasonable means for acquiring the information have been considered and ruled out.

Now the term "unavoidable circumstances" has not been defined under the Telegraph Rules, Telegraph Act, any other legislation, or judgments by courts of law. As a result, there exists no objective standard to determine whether a given situation qualifies as an unavoidable circumstance. This raises the very pertinent question: who decides whether a circumstance is unavoidable and how?

Setting aside this unresolved ambiguity in procedure, Rule 419A stipulates another exception to the general rule. In *emergent cases*, where procuring a lawful order is itself infeasible – either due to remoteness of location, or for operational reasons, interception may be carried out with the prior approval (as distinct from lawful order) of the Head or the second senior most officer of the authorized Law Enforcement Agency at the Centre, or officers authorized in this behalf – not below the rank of Inspector General of Police – at the States.

This exception to the general rule operates at the implementational level of interception, and says that if it is not possible to procure a lawful order for either of the listed reasons, the interception process may commence even without a lawful order as long as it is approved by a senior official as specified of the intercepting agency. However, when

interception is carried out in this fashion, the relevant sanctioning authority – be it a Union/State Home Secretary (or possibly a Joint Secretary) – must be informed of the fact within 3 working days, and the lawful order itself must be procured within 7 working days. Failing this, all interception must cease from the 8th day, until a lawful order is procured from the concerned sanctioning authority.

Rule 419A also states that a lawful order may be issued only once all other reasonable means for acquiring the information have been considered and ruled out. Any order so issued will remain in force for a period of 60 days from the date of issue, unless revoked earlier. Though the order may subsequently be renewed if necessary, no order will remain in force for more than a sum total of 180 days. All lawful orders must further contain:

• reasons behind the order, and;

• name and designation of the authority to whom the intercepted information is to be disclosed, and;

• a statement to the effect that the use of intercepted information will be subject to Section 5(2) of the Telegraph Act.

When a lawful order is issued by any of the concerned authorities, a copy must be forwarded within 7 working days to the respective Central/State Review Committee, which has been constituted by the Central/State Government under Rule 419A for the sole purpose of reviewing lawful orders. The constitution of Review Committees, though entirely Executive in nature, differs depending on whether it is a Central or State Review Committee. A Central Review Committee will consist of the Cabinet Secretary as Chairman, and the Secretary to the Government of India In-charge, Legal Affairs and the Secretary to the Government of India, Department of Telecommunications as Members. A State Review Committee on the other hand, will consist of the Chief Secretary as Chairman, and the Secretary Law/Legal Remembrancer In-charge, Legal Affairs and a Secretary to the State Government (other than the Home Secretary) as Members.

Review Committees will meet at least once in 2 months and determine if the lawful orders placed before them are in accordance with Section 5(2) of the Telegraph Act. When a Committee is of the opinion that a lawful order is violative of Section 5(2), it may set aside the order and ask that all copies of information intercepted under that particular order be destroyed.

2.1.2 Interception process under Rule 419A

Now that we have seen how a lawful order is procured and reviewed under Rule 419A, we turn to the process of interception itself. Procedure in this regard must be adhered to at all times, even if interception is undertaken in unavoidable or emergent circumstances.

The actual ground-level interception of communications over telephones will be carried out by various Law Enforcement Agencies such as the Intelligence Bureau and the Research and Analysis Wing, which have been specifically authorized

to this effect by the Government. However, the identities of agencies so authorized are not disclosed to the public for security reasons.

In any case, as per Rule 419A, all intercepting agencies will designate one or more nodal officers to authenticate and relay requisitions for interception between the agencies and Telecommunications Service Providers. These nodal officers will be senior officials of the agencies, not below the rank of (Additional) Superintendent of Police or equivalent. The TSPs in turn will designate two senior officials as nodal officers to receive and handle requisitions. Requisitions (which will include lawful orders authorizing interception) will be delivered to nodal officers of the respective TSPs by officers not below the rank of Sub-Inspector of Police, and the nodal officers will issue letters of acknowledgement to the relevant intercepting agencies within 2 hours of their reception.

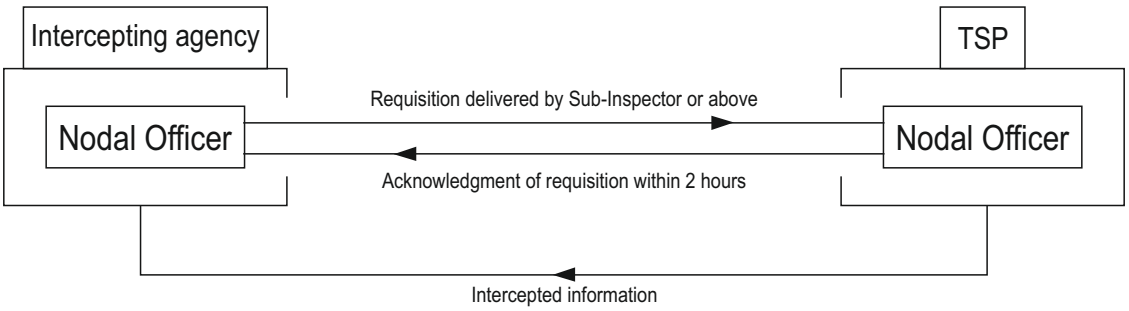

Fig. 2 – Interception process

Here ends the procedure detailed by Rule 419A with respect to the interception process. Internal protocol to be followed by both intercepting agencies and TSPs in handling requisitions for interception,

which presumably explains how intercepted information finds its way to the intercepting agencies, are further enumerated by periodic guidelines or notifications issued by the Central Government in the form of Standard Operating Procedures. However,these SOPs are kept out of public reach for security reasons, thereby ensuring that none other than those directly involved in the interception process have a comprehensive idea of the end-to-end procedure. An RTI request filed by SFLC.in seeking a copy of the latest of such SOPs was denied by the Department of Telecommunications, claiming exemption under Section 8(1)(a) of the RTI Act, which exempts the disclosure of information that may prejudicially affect national security.

Rule 419A does nevertheless go on to lay down certain procedural safeguards aimed at preventing misuse of intercepted information.

For starters, officers authorized to intercept are required at all times to maintain records that contain the intercepted information itself, particulars of interceptees, particulars of those to whom intercepted information has been disclosed, number of copies of intercepted information created, mode of creating said copies, date of destruction of said copies and duration for which the lawful order remained in force. TSPs in turn, are to put in place adequate and effective internal checks in order to ensure that unauthorized interception does not take place, and that extreme secrecy is maintained, and utmost care and precaution taken in the interception process. Further, TSPs are made responsible for the actions of their employees, and established violations of relevant license[3] clauses will result in action being taken against TSPs under the Telegraph Act, and this may even extend to revocation of their licenses. Last, but certainly not the least, all records pertaining to intercepted information are to be destroyed by sanctioning authorities and intercepting agencies every 6 moths, unless they (likely) need to be retained for "functional requirements". Similarly, TSPs are to destroy all such records 2 months after ceasure of interception, and are required to maintain extreme secrecy in doing so.

2.2 Internet

Provisions dealing with Internet surveillance may be found interspersed throughout the **Information Technology Act, 2000** and several Rules made thereunder.

But before looking at the enabling provisions themselves, a distinction must be made between "Internet data" and "Internet meta-data" – the two broad categories of electronic data, whose surveillance is provisioned by the below statutory clauses. The term "Internet data" connotes the core contents of data-packets transmitted between a user-end device and the host-server in which information accessed by the user resides. This would include the contents of

3 This refers to the service licenses granted to service providers by the Department of Telecommunications, which govern the general, technical, financial, operational and security conditions under which service providers must operate.

websites browsed, e-mails sent/received, chat-logs and so on. "Internet meta-data" on the other hand, signifies particulars of Internet data *apart from its core-contents*. This would include information such as date and time of transmission, duration for which data was transmitted and location from/to which data was transmitted.

With that out of the way, **Section 69** of the IT Act, modeled extensively after Section 5(2) of the Telegraph Act, allows the Government to engage in surveillance of Internet data. It reads:

> (1) *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 the incitement to the commission of any cognizable offence relating to the above or for the investigation of any offence, it may, subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource.*
>
> (2) *The procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed.*
>
> (3) *The subscriber or intermediary or any person in-charge of the computer resource shall, when called upon by any agency referred to in sub-section (1), extend all facilities and technical assistance to -*
>
> (a) *provide access to or secure access to the computer resource generating, transmitting, receiving or storing such information; or*
>
> (b) *intercept, monitor, or decrypt the information, as the case may be, or;*
>
> (c) *provide information stored in computer resource*
>
> (4) *The subscriber or intermediary or any person who fails to assist the agency referred to in sub-section (3) shall be punished with imprisonment for a term which may extend to seven years and shall also be liable to fine.*

As can be seen, Section 69 in provisioning surveillance of Internet data, draws much of its language from Section 5(2) of the Telegraph Act. The former, however, makes three notable departures from the latter. Firstly, Section 69 dispenses with the all-important *sine qua non* found under Section 5(2), *viz.* the occurrence of a public emergency or interest of public safety. Interception, monitoring, and decryption of Internet data under Section 69 is therefore not predicated on the prevalence of either pre-requisites, and this considerably widens the Govern-ment's

surveillance avenues when it comes to Internet data. Secondly, the grounds under Section 69, in the interest of which interception etc. of Internet data may be undertaken, is slightly larger in number and significantly greater in scope, as evidenced by the comparative table given below:

Grounds under Section 5, Indian Telegraph Act	Grounds under Section 69, Information Technology Act
Sovereignty/integrity of India	Sovereignty/integrity of India
-	Defence of India
Security of the State	Security of the State
Friendly relations with foreign States	Friendly relations with foreign States
Public order	Public order
Prevention of incitement to the Commission of any offence	Prevention of commission of any cognizable offence relating to the above
-	Investigation of any offence

Table 1 – Grounds for interception under Section 5(2), Telegraph Act and Section 69B IT Act

Lastly, unlike Section 5(2), Section 69 imposes an obligation on those from whom Internet data is demanded (Internet Service Providers, for instance) to provide all assistance to the intercepting agency, failure to comply with which may result in incarceration for up to *7 years* and fines.

With surveillance of the Internet data thus provisioned by Section 69, **Section 69B** in turn deals with surveillance of Internet meta-data. It reads:

> 1. *The Central Government may, to enhance Cyber Security and for identification, analysis and prevention of any intrusion or spread of computer contaminant in the country, by notification in the official Gazette, authorize any agency of the*

Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource.

2. *The Intermediary or any person in-charge of the Computer resource shall when called upon by the agency which has been authorized under sub-section (1), provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating, transmitting, receiving or storing such traffic data or information.*

3. *The procedure and safeguards for monitoring and collecting traffic data or information, shall be such as may be prescribed.*

4. *Any intermediary who intentionally or knowingly contravenes the provisions of subsection (2) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.*
Explanation: For the purposes of this section,

i) *"Computer Contaminant" shall have the meaning assigned to it in Section 43*

ii) *"traffic data" means any data identifying or purporting to identify any person, computer system or computer network or location to or from which the communication is or may be transmitted and includes communications origin, destination, route, time, date, size, duration or type of underlying service or any other information.*

Section 69B allows the collection and monitoring of meta-data – cloaked as "traffic data" - for the twin purposes of enhancing cyber security and tackling computer contaminants. The term "cyber security" has been defined under Section 2(1)(nb) of the IT Act as the protection of information or devices from unauthorized access, use, disclosure, disruption, modification or destruction, and the term "computer contaminants" as per Section 43 of the IT Act denotes malicious software such as computer viruses. Both grounds for invocation of Section 69B are visibly broad in ambit, and essentially allow surveillance of meta-data at any given point of time.

The procedure to be followed while invoking Sections 69 and 69B are laid down under the **Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009**, and the **Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009**. The procedure outlined by these Rules are near-identical replications of the procedure under Rule 419A of the Telegraph Rules, and their reiteration here is therefore unnecessary for the purpose of this report. It would suffice to keep in mind that Internet surveillance is governed by the same broad procedural framework as telephone surveillance.

While Sections 69 and 69B together set the stage for direct surveillance of Internet networks, more provisions of the IT Act allow indirect surveillance i.e. they allow

the Central/State Governments and their agents such as the Controller of Certifying Authorities and police officers to collect "information" under specified circumstances. In the absence of clarifications on the nature of information that can be collected, these provisions serve as alternate means to collect Internet data and meta-data when surveillance by means of Sections 69 and 69B may not be feasible:

• **Section 28** of the **Information Technology Act** allows Government officials to access any electronic data while investigating contraventions of the Act and Rules or regulations made under the Act. The Section states that the Controller of Certifying Authorities (CCA) or any authorized officer may direct production of information towards investigating contraventions of the Act or connected Rules and regulations. It confers on them the powers of Income-tax authorities as under *Chapter XIII of the Income Tax Act, 1961* for the purposes of such investigation. Chapter XIII of the Income Tax Act awards the authorities significant powers of investigation, including the power to compel production of information stored electronically. Thus, the CCA in effect has the same authority under Section 28, provided such authority is exercised in the course of investigating a contravention of the IT Act.

In 2011, the CCA had imposed a fine on Yahoo! To the tune of Rs. 11 lakhs for its refusal to provide user information requested under Section 28. An interim order staying the fine was issued by the Delhi High Court in 2011, and a final order setting aside the fine was issued in February 2014.

Further, a Right to Information request filed by SFLC.in revealed that the CCA had made 73 requests for information in 2011 under Section 28.

• **Section 29** of the **Information Technology Act** provides the CCA or authorized officers with the power to access computers and their data on a *reasonable cause* to suspect contravention of Chapter VI of the Act. Chapter VI deals with regulation of Certifying Authorities and contains a number of provisions, whose contravention could be easily and reasonably suspected. Since no framework for the access of computers and data has been prescribed by the Section, it is frighteningly easy for Section 29 to be wrongfully invoked to access private user information from Certifying Authorities.

• **Rule 6** of the **Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011**, says that though a body corporate is disallowed from disclosing sensitive personal data or inform-

ation to third parties without the prior consent of the provider of the information, it may disclose the same to Government agencies mandated under law without prior consent for the purpose of identity verification, prevention, investigation of offences etc. It further states that any sensitive personal data or information shall be disclosed to third parties by an order under law, presumably without prior consent of the provider.

• **Rule 3(7)** of the **Information Technology (Intermediaries Guidelines) Rules, 2011**, requires that intermediaries such as ISPs and on-line portals must provide information or any assistance to authorized Government agencies for the purpose of identity verification, prevention or investigation of offences etc., when asked to do so by a lawful order. There is some confusion here regarding the term 'lawful order' since the Rule uses it interchangeably with the term 'request in writing'. This seemingly implies that a 'lawful order' as envisioned under the Rule is nothing more than a written letter from authorized Government agencies, which does not bear adequate force of law. As a result, the process of directing the production of information under Rule 3(7) is inordinately simplified, and this is evident in general practice. The constitutionality of this provision was challenged by Yahoo in a Writ Petition[4] filed before the Delhi High Court, following the imposition of a hefty fine for refusal to provide information to the CCA under Section 28 of the IT Act. Though the fine itself was set aside by the Court, larger questions of law such as the constitutionality of Rule 3(7) were left undecided. The Rule has also been challenged before the Supreme Court in the cases of Rajeev Chandrashekhar v. UoI[5] and MouthShut.com v. UoI[6] as being violative of the citizens' right to privacy. Both cases are currently pending before the Supreme Court, awaiting judgement.

• **Rule 7** of the **Information Technology (Guidelines for Cyber Cafe) Rules, 2011**, states that an officer authorized by the registration agency, is authorized to check or inspect the cyber cafe and the computer resource or network established therein at any time for the compliance of these rules. The cyber cafe owner shall provide every related document, registers and any necessary information to the inspecting officer on demand. This is especially interesting, considering that cyber cafes are also classified as intermediaries under the IT Act. Thus, Rule 7 can be used to access personal information from cyber cafes including Internet histories

4 W.P.(C).No. 6654/2011
5 W.P.(C).No. 23 of 2013
6 W.P.(C).No. 217 of 2013

and other user-related information.

Apart from the IT Act and Rules, **Section 91** of the **Code of Criminal Procedure, 1973** (CrPC) says that any Court or officer in charge of a police station may require the production of any document or 'other thing' if it is considered necessary for the purposes of an investigation, inquiry, trial or any other proceeding under the CrPC. Since this is the legislation which the police authorities are familiar with, it is often found that requisitions sent to intermediaries directly by the police often ask for information based on Section 91. For instance, a vernacular blog *bodhicommons.org* was issued a notice in February 2013 under Section 91 based on a complaint made by a regional media house *Mathrubhumi*, where the blog was asked to remove an allegedly defamatory post containing discussions on unfair labour practices at *Mathrubhumi*. The notice also directed bodhicommons to furnish registration details of the URL (sic) from which the offending post was originally made. Again, a consumer review website *mouthshut.com* was issued notices under Section 91 demanding identification details regarding the up-loaders of several unfavourable reviews found on the website.

Thus the above-mentioned provisions of law collectively enable the Government and its agents to surveil India's telephone and Internet networks on a variety of grounds. However, these are not the only sources from where such authority is derived. In addition to legislations, surveillance-enabling clauses/conditions are also found across several service license agreements, which are discussed in the following pages.

Since this is the legislation which the police authorities are familiar with, it is often found that requisitions sent to intermediaries directly by the police often ask for information based on Section 91.

3. Enabling License Agreements

Having seen the surveillance-enabling provisions found across Indian legislations, we turn to more enabling clauses – found this time around in license agreements between the Department of Telecommunications (DOT) and communications service providers. The DOT is an executive organ of the Ministry of Communications and Information Technology, and is the prime regulator of Indian communications service industry. The aforementioned license agreements in their various iterations, govern provision of the following services:

- Fixed-line telephones
- Cellular/mobile telephones
- Internet
- Satellite communications
- Two-way radios
- Private leased circuits

These license agreements are essentially what allow service providers to conduct their businesses in India, and accordingly they detail the various general, commercial, financial, operational, technical and security conditions under which they must operate. Licensees are under a legal obligation to abide by all said conditions, failing which their licenses may be revoked. But before getting into the surveillance-enabling clauses, some background information on the license agreements themselves is in order.

Prior to 2003, the Indian communication service licensing regime was fragmented into multiple individual licenses, with separate licenses for each kind of communication service mentioned above. However, it was recognized in the New Telecom Policy (NTP) of 1999 that the ongoing convergence of markets and technologies called for a realignment of this licensing model. While technology was busy blurring the lines of differentiation among conduit systems, various service providers were already entering one another's markets. In view of such fundamental shifts in the telecom service paradigm, the Telecom Regulatory Authority of India (TRAI) recommended the consolidation of the fragmented individual licenses into a single unified model. Though the key objective of the proposed unified licensing model was to encourage free growth of new applications and services leveraging the technological advancements, it also had the following ancillary objectives:

- Simplification of licensing procedure
- Ensuring flexibility and efficient utilization of resources
- Encouraging efficient small service providers to cover niche areas, particularly rural and remote areas where telecom penetration was insufficient
- Ensuring easy entry, level playing field and 'no-worse-off' situation for existing service providers

With these objectives in mind, the consolidation of licenses was kicked off in 2003 in two phases:

- The first phase introduced the Unified Access Service License (UASL) merging license agreements covering provision of fixed-line and cellular/mobile telephone telephone services.

- The second phase introduced the Unified License (UL) as part of the New Telecom Policy of 2012, which merged *all* service licenses into one umbrella license.

However, migration to the new UL has been prescribed on a voluntary basis and thus, while subscribers to the erstwhile individual licenses have almost entirely migrated to the UASL, migration to the UL is still ongoing with only two service providers – Sistema Shyam Teleservices (operating under the brand name MTS) and Reliance Jio Pvt. Ltd. - currently subscribed to the UL.

Since the scope of this report is Indian surveillance of *mainstream* communications, its focus will be on the license agreements currently governing provision of fixed-line/mobile telephone and internet services, namely:

- Unified Access Service License (UASL)

- Internet Service License (ISL)

- Unified License (UL), particularly Chapters VIII and IX of Part II, which incorporate the above-two licenses into the UL

All of the above-mentioned license agreements require their licensees to furnish 'all necessary means and facilities as required' for the application of Section 5[7] of the Indian Telegraph Act[8]. Licensees must also provide in the interests of security, 'suitable monitoring equipment' as per the requirement of the DOT or LEAs[9]. The specific orders or directions from the Government issued under such conditions (i.e. in the interests of security) are also applicable[10]. Further, licensees are obliged to provide all tracing facilities to trace nuisance and obnoxious/ malicious communications passing through their networks, when such information is required for investigations or detection of crimes, and in the interest of national security[11]. They must also provide 'necessary facilities' depending upon the specific situation at the relevant time, to counteract espionage, subversive act, sabotage or any other unlawful activity[12].

Thus under the afore-mentioned clauses, licensees may be asked to provide surveillance equipment in any *one* of the following scenarios:

- Situations where Section 5 of the Indian Telegraph Act is applicable

- In the interests of (national)

7 See p. 3
8 Clause 32.2, UASL; Clause 35.2, IL; Condition 32.2, Part I, UL
9 Clause 41.13, UASL; Clause 34.4, IL; Condition 39.12, Part I, UL
10 Ibid.
11 Clause 40.4, UASL; Condition 38.2, Part I, UL
12 Clause 41.1, UASL; Condition 39.1, Part I, UL

security

• For the investigation/detection of crimes

• To counteract:

  • Espionage
  • Subversive acts
  • Sabotage
  • Any other unlawful activity

Terms such as national security, espionage, subversive acts and sabotage are not defined anywhere in the license agreements, enabling the Government to call for the installation of surveillance equipment with no accompanying obligation to clearly outline reasons for the same.

It is also interesting to note that the nature of surveillance equipment to be provided is not mentioned under the licenses. Instead, open-ended terms such as 'necessary means and facilities', 'suitable monitoring equipment' and 'tracing facilities' are liberally employed, which may signify virtually *any* surveillance equipment depending on the need of the hour and the state of technological progress.

That being said, the licenses do however specify the following details regarding surveillance systems, depending on their functionality:

3.1 Telephone tapping

Designated Central/State Government officials, apart from the DOT and its nominees, may access telephone-tapping systems installed into the licensees' networks.[13] Whereas the hardware belonging to such systems at the licensees' end, as well as all related software must be engineered, installed and maintained by the licensees at their own cost,[14] the cost of user-end hardware and leased line circuits to the monitoring centers will be borne by the respective Government agency. These monitoring centres may be located in the Government agencies' premises or in the premises of the licensees.[15] In the latter case, licensees should extend all support in this regard including Space and Entry of the authorized security personnel.[16]

Further, Licensees should make arrangements for monitoring simultaneous calls by Government security agencies.[17] The number of simultaneous calls to be monitored has been given to be 480, with at least 30 for each of the 10 currently designated security agencies.[18] Identities of the specific designated agencies are unknown at this time as this information is provided directly to the service providers and agencies in the form of periodic (publicly inaccessible) guidelines. Additionally, each of the licensees' Mobile Switching Centres must have the capacity to provision at least 3000 numbers for monitoring.[19]

13 Clause 41.16, UASL; Condition 8.2, Part II, Chapter VIII, UL
14 Ibid.
15 Clause 41.16, UASL; Condition 8.2, Part II, Chapter VIII, UL
16 Ibid.
17 Supra. 7
18 Supra. 9
19 Supra. 9

Along with the monitored calls, the following records must also be made available:[20]

- Called/calling party mobile /PSTN numbers
- Time/date and duration of interception
- Location of target subscribers. For the present, Cell ID should be provided for location of the target subscriber. However, Licensor may issue directions from time to time on the precision of location, based on technological developments and integration of Global Positioning System (GPS) with Cellular Network, which shall be binding on the licensee.
- Telephone numbers if target subscriber has invoked any call-forwarding features
- Data records for even failed call attempts
- CDR (Call Data Record) of Roaming Subscriber

3.2 Surveillance of Internet data

Clauses dealing with surveillance of Internet data see some variation between the ISL and the UL.

3.2.1 Obligations of ISPs under ISL

> Under the ISL, ISPs are required to maintain copies of all packets originating from their equipment such as modems or routers located on the customers' premises, and these must be available in real time to the Telecom Authority

Under the ISL, ISPs are required to maintain copies of all packets originating from their equipment such as modems or routers located on the customers' premises, and these must be available in *real time* to the Telecom Authority[21].[22] Further, every international gateway location and/or ISP node with a router/switch having an outbound capacity of 2 Mbps or more must be equipped with a monitoring center at the cost of the ISP.[23] 'Suitable monitoring systems' must also be set up by ISPs carrying Internet telephony traffic through their internet gateways and/or ISP nodes at their own cost, as per the requirement of the security agencies, and the cost of maintenance of the monitoring equipment and infrastructure at the monitoring center located at the premises of the licensee shall be borne by the ISP.[24] For a national ISP or an ISP having multiple nodes/points of presence, a central monitoring center would be acceptable. However in such a case, the ISP should demonstrate to the DOT that all routers/switches are accessible from the

20 Clause 41.17, UASL; Condition 8.3, Part II, Chapter VIII, UL
21 Denotes the Director General, Telecommunications, Government of India and includes any officer empowered by him to perform all or any of the functions of the Telegraph Authority under the Indian Telegraph Act, 1885 or such other authority as may be established by law
22 Supra. 13
23 Clause 34.27, ISL
24 Ibid.

central monitoring center. Moreover, the ISPs should inform the DOT of every change that takes place in their topology/configuration, and demonstrate that all routers/switches continue to be accessible from the central monitoring center.[25] At locations where the ISP node has a router/switch with an outbound capacity of less than 2 Mbps, monitoring equipment will be provided by the security agencies.[26]

3.2.2 Obligations of ISPs under UL

The UL one the other hand requires ISPs to provide copies of customers' packets to the DOT or security agencies, as opposed to the Telecom Authority.[27] Further, 'suitable monitoring systems' for internet traffic – including internet telephony – flowing through the licensees' internet gateways/ISP nodes are to be set up by the licensees at their own cost as per the requirement of the DOT or security agencies.[28] The cost of maintenance of the monitoring equipment and infrastructure at the monitoring centers located at the premises of the licensees shall be borne by the licensees.[29] Licensees, while providing downstream Internet bandwidth to an ISP, should ensure that all the traffic of such ISPs passing through their networks can be monitored in the networks of the licensees.[30] However, licensees having upstream bandwidth from multiple service providers may be mandated to install monitoring systems at their ISP nodes as per the requirement of security agencies. In such cases, upstream service providers are not required to monitor this bandwidth.[31] The UL also makes the option of having one centralized monitoring center as opposed to multiple centers available to all ISPs having multiple nodes/points of presence, irrespective of whether they are national or international ISPs.

3.3 Surveillance of Internet metadata

Both the UASL and the UL require their licensees to archive all commercial records/Call Data Records/Exchange Data Records/IP Data Records with regards to communications exchanged in their networks for a period of one year for security reasons.[32] While the specific contents of these Data Records are unspecified, they may be destroyed thereafter unless otherwise directed by the DOT.[33] Interestingly though, the ISL in particular makes no mention of IP Data Records. However, IP Data Records would need to be archived by ISPs subscribed to the UL.

Further, licensees operating under the UASL and UL must be able to provide the geographical location of any subscriber (Base Transceiver Station location, and location details including latitude &

25 Supra. 23
26 Supra. 19
27 Condition 7.3, Part II, Chapter IX, UL
28 Condition 8.1.1, Part II, Chapter IX, UL
29 Ibid.
30 Condition 8.2, Part II, Chapter IX, UL
31 Condition 8.3, Part II, Chapter IX, UL
32 Clause 41.23, UASL;
33 Ibid.

longitude details) on request by the DOT or its authorized agencies.[34] They must also provide location details of mobile customers in licensed service areas as per the below-mentioned accuracy and time frame from the effective date of licenses:[35]

Accuracy in percentage							
Distance in meters	**Urban (More than 1 million mobiles in a municipal limit)**		**Sub-urban and rural**			**Remote**	
	1 year	2 years	1 year*	2 years	3 years	2 years	3 years
50	30	50					
100	60	75		50	60		-
300	80	95	50	60	70	50	60
500			60	70	80	60	70

Table 2 – Accuracy and time frame for collection of location details

To start with, these details need be provided only for specified mobile numbers - however, within a period of 3 years from effective date of license, they shall be part of CDR for *all* mobile calls.[36] Also, depending on technological development, these limits of accuracy can be modified by the DOT at any time.[37] Once again, the ISL makes no mention of location details in particular, but they would need to be provided by ISPs operating under the UL.

However, ISPs operating under the ISL are required to maintain logs of all users connected and the service they are using (mail, telnet, http etc.). They must also log every outward login or telnet through the connected users' computers. These logs must be available in *real time* to the Telecom Authority, and anonymous

34 Clause 41.26(x), UASL; Condition 39.23(x), Part I, UL
35 Clause 41.12, UASL; Condition 8.5, Part I, UL
36 Supra. 29
37 Ibid.

logins by users are not allowed.[38] The UL further mandates ISPs to maintain CDR/IPDR for Internet including Internet Telephony Service for a minimum period of one year.[39] Parameters of IPDR must be maintained as per the instructions issued by the DOT from time to time.[40] ISPs operating under the UL are also to maintain log-in/log-out details of all subscribers for services provided such as internet access, e-mail, Internet Telephony, IPTV etc. These logs shall again be maintained for a minimum period of one year.[41]

This just about sums up the license agreement clauses that provision direct surveillance of the nation's communication networks. As previously mentioned, the specific surveillance systems/ technologies to be employed by service providers are left unmentioned, and the license agreements settle instead for delineating the nature of information to be supplied and the manner in which they must be supplied. The Government agencies are then free to retrieve such information using the surveillance systems of their choice, depending on the state of technological progress and the availability of and need for said systems.

It is worth mentioning that the license agreements, apart from provisioning direct surveillance of communications, also contain certain provisions that quietly facilitate the Government's information gathering efforts. For instance, all licensees under all licenses discussed here are prohibited from employing bulk encryption equipment in their networks. Any encryption equipment connected to their networks for specific requirements need to be pre-evaluated and approved by the DOT.[42] The ISL in particular states that individuals, groups and organizations are permitted to use encryption only up to 40 bit key length in the symmetric key algorithms or its equivalent in other algorithms without obtaining permission from the DOT. If encryption equipment higher than this limit are to be deployed, they must obtain prior written permission of the DOT and deposit the decryption key, split into two parts, with the DOT.[43]

That said, we now move on to the actual surveillance systems employed by the Government of India – both the currently functional systems, as well as those in the pipeline.

38 Clause 34.8, ISL
39 Condition 7.1, Part II, Chapter IX, UL
40 Ibid.
41 Condition 7.2, Part II, Chapter IX, UL
42 Clause 39.1, UASL; Clause 2.2(vii), ISL; Condition 37.1, Part I, UL
43 Clause 2.2(vii), ISL

4. Functional Surveillance Mechanisms

Backed by legislations and license clauses, a host of surveillance systems perform the task of keeping a close tab on India's communication networks. Here we take a look at what is currently known regarding these systems – including their functionality and modes of operation. As a word of caution, said surveillance systems have been kept under tight wraps by the Government citing various security concerns, and reliable information on them is extremely difficult to come by in the public domain. While every effort has been made to source the facts detailed below from the most reliable of the available sources, they must nevertheless be regarded as involving a certain amount of speculation unless otherwise mentioned.

4.1 Lawful Intercept and Monitoring systems

Lawful Intercept and Monitoring systems – also known simply as Lawful Interception Systems (LIS) – generally refer to any legally approved surveillance system, public or private, that operate in a jurisdiction at a given point of time. However, in the context of this report, they may be understood to signify the interception/monitoring systems installed into the networks of TSPs/ISPs under the authority of the license agreements discussed in Chapter III. From a perusal of the relevant license clauses, it may be gathered that the collective body of LIM systems will be able to perform the following broad tasks:

- Intercept fixed-line/mobile/ internet telephone calls
- Log and provide real time access to the entirety of Indian internet traffic
- Maintain and provide access to meta-data i.e. Call Data Records/ Exchange Data Records/IP Data Records relating to the above, including, but not limited to the location of subscribers

Though the details on how these tasks are accomplished remain rather sketchy, a broad idea of the technology that powers LIM systems may be gleaned from the product portfolios of surveillance technology companies operating in India, who manufacture and distribute various lawful interception solutions aimed primarily at LEAs. Considering that selling surveillance technology to LEAs is clearly a viable business model, and that several key players from this industry have set up bases in India, a reasonable assumption can safely be made that such technology powers India's LIM systems at least in part. An RTI request filed by SFLC.in revealed a list of 26 companies that had expressed interest in placing bids on a tender calling for internet monitoring systems floated by the office of the Director General of Police, Logistics & Provisioning, New Delhi. Said companies are:

- Alcatel-Lucent India
- Agilis Information Technologies International
- Appin Software Security

- Aqsacom India
- ClearTrail Technologies
- Electronics Corporation of India Ltd., Information Technology & Telecom Division
- HCL Infosystems
- Hewlett-Packard India Sales
- Innefu Labs
- Intelligent Communication Systems India
- ITI
- Kommlabs Dezign
- Law Abiding Technology
- Narus Networks
- Netsweeper India
- NICE Systems
- Pyramid Cyber Security and Forensics
- Siemens Information Systems
- Span Technologies
- Span Telecom
- SS8 Network
- Telecommunications Consultants India
- Vehere Interactive
- Verient Systems India
- Vox Spectrum
- Xalted Information Systems

It can thus be safely definitively inferred that these 26 domestic as well as international companies already sell/are interested in selling internet surveillance technology to Indian LEAs. However, a look at their product portfolios – several of which have incidentally been published by WikiLeaks as part of *The Spy Files* initiative – will tell us that some of them also offer far more potent surveillance technologies including phone interception, social network analysis, and data-mining and profiling. However, there are no definite indicators as to which of the above-mentioned companies are active suppliers of surveillance equipment to Indian LEAs, and by extension, which specific technologies are in fact deployed.

... it is important to note that the operation of all LIM systems are bound by the procedural guidelines laid down by Section 5 of the Indian Telegraph Act read with Rule 419A of the Indian Telegraph Rules

That said, it is important to note that the operation of all LIM systems are bound by the procedural guidelines laid down by Section 5 of the Indian Telegraph Act read with Rule 419A of the Indian Telegraph Rules, where interception may only be

conducted in specified circumstances, and in pursuance of a lawful order issued by the competent authority on a case by case basis. The license agreements further mention 10 LEAs authorized to access LIM systems, though their identities are undisclosed. A report published by a national newspaper in June 2013[44] refer to the following nine LEAs as being authorized to "intercept and monitor citizens' calls and emails, under the guidelines laid down by the Supreme Court, The Indian Telegraph Act 1985, Rule 419(A) and other related legislation": Central Board of Direct Taxes (CBDT), Central Bureau of Investigation (CBI), Defense Intelligence Agency (DIA), Directorate of Revenue Intelligence (DRI), Enforcement Directorate (ED), Intelligence Bureau (IB), Narcotics Control Bureau (NCB), National Investigation Agency (NIA), Research and Analysis Wing (RAW), Military Intelligence of Assam and Jammu and Kashmir, and the Home Ministry. While by no means is this conclusive proof that these 9 LEAs are part of the 10 authorized LEAs mentioned in the license agreements, it would at least serve as an indicator of the nature of LEAs authorized in the usual course to conduct communications surveillance.

Thus, the majority of current Indian communications surveillance may be understood to be carried out by this existing framework of LIM systems. However, a number of additional surveillance systems in varying stages of development are currently in the works, including:

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

Unlike the current framework of LIM systems, a good portion of which may be privately sourced, these newer surveillance systems are engineered almost exclusively by various public R&D establishments such as the Defence Research and Development Organization (DRDO) or the Centre for Development of Telematics (C-DOT), and will work in tandem with the existing set up.

4.2 Centralized Monitoring System

Plans to set up the CMS were first announced in a November 2009 press release by the Press Information Bureau, where the then UPA Government notified its proposal to set up a centralized system to monitor communications on mobile phones, landlines and internet in the country.[45] As per the press release, the CMS was envisaged by the DOT to 'strengthen the security environment in the country'. It was said that with the CMS, the following inherent problems in the present system would be overcome:

- Easy compromise of secrecy due to manual intervention
- Considerable delay in interception process

44 http://www.thehindu.com/news/national/indias-surveillance-project-may-be-as-lethal-as-prism/article4834619.ece , accessed on December 14, 2013

45 http://pib.nic.in/newsite/erelease.aspx?relid=54679 , accessed on February 5, 2014

Additionally, the CMS was touted as having the following features:

- Central and regional database that will help Law Enforcement Agencies in interception and monitoring
- Direct Electronic Provisioning of target numbers by Government agencies without any manual intervention from the Telecom Service Providers
- Filters and alert creation on target numbers
- Call Data Records analysis and data mining on CDRs to identify call details, location details etc. of the target numbers
- R&D in related fields for continuous upgradation of the CMS

That said, it is important to note however that the CMS isn't a surveillance system *per se,* since the actual interception and monitoring of communications will still be carried out by the pre-existing framework of LIM systems. The CMS will primarily function in the capacity of an automated system of accessing information that has already been intercepted by LIM systems. For this purpose, it will have central and regional databases that will store intercepted data and provide access to LEAs authorized to use the CMS. But the CMS will be a massive step-forward from the existing surveillance framework, mainly due to its elimination of manual components from the interception chain of command. This automation of the interception process has two implications:

- LEAs using the CMS will no longer need to approach telecom/ internet service providers on a case-by-case basis to retrieve intercepted information
- The intercepted information will be delivered to LEAs instantaneously

The CMS will comb through information gathered to look for key words or phrases that have been flagged as indicative of unlawful activity and alert LEAs when such words/phrases are detected. Additionally, it will have CDR analysis and data-mining capabilities, which means it will also analyze meta-data to build speculative profiles of targeted individuals.

While it is thus clear that the CMS will have significant surveillance capabilities once fully functional, it is not intended to replace the existing LIM systems. The CMS' role will be restricted to the elimination of manual components in the information retrieval process and the consequent analysis of said information. To this end, the existing LIM systems will be linked to Information Store and Forward (ISF) servers belonging to the CMS, which will in turn be linked to the databases of CMS' Regional Monitoring Centers (RMC), which will finally feed into the CMS' central database, from where the

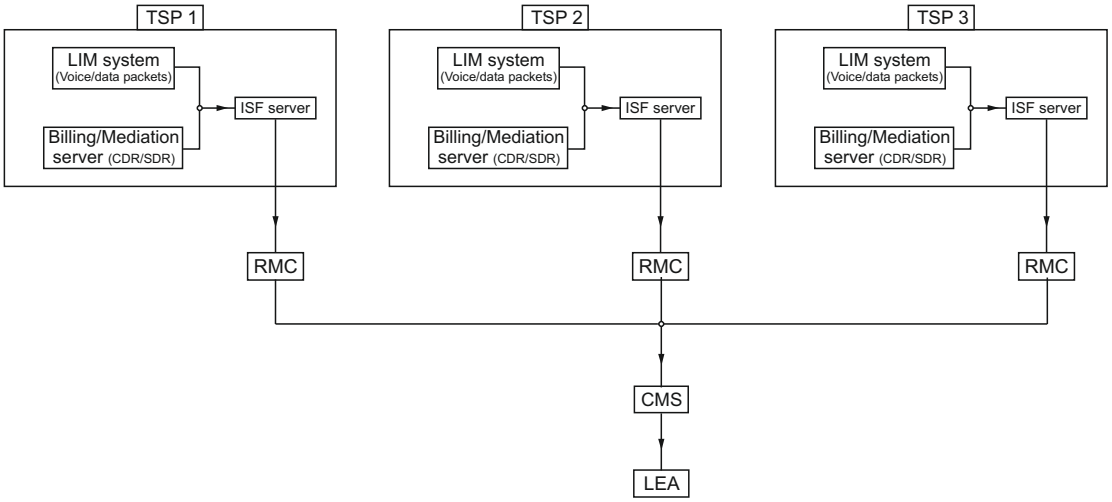

Fig. 3 – Collection of Information under Centralized Monitoring System

information will be accessed by authorized LEAs.[46]

In addition to the content of intercepted communications, the CMS will also have access to communications meta-data i.e. CDR and IPDR, which will be secured on multiple E1 leased lines through service providers' billing/ mediation servers.[47] In 2013, amendments were made to the Unified Access Service License and Unified License in order to connect the existing monitoring centers to the CMS network. Said amendments require service providers to provide dark optic fiber connectivity at their own cost up to the nearest point of presence of the CMS network. In case dark optic fiber connectivity is not readily available, (regular) optic fiber connectivity must be provided with 10 Mbps bandwidth upgradeable to 45 when required, but the switch to dark optic fiber must be made at the earliest.

As of June 2013, the following Government agencies are rumored to have been authorized to make intercept requests through CMS: Central Board of Direct Taxes (CBDT), Central Bureau of Investigation (CBI), Defense Intelligence Agency (DIA), Directorate of Revenue Intelligence (DRI), Enforcement Directorate (ED), Intelligence Bureau (IB), Narcotics Control Bureau (NCB), National Investigation Agency (NIA), Research and Analysis Wing (RAW), Military Intelligence of Assam and Jammu and Kashmir, and the Home Ministry.[48] While a majority of the RTIs filed by various organizations and individuals seeking to uncover information on the working of CMS were denied as the information was claimed to be protected under Section 8(1)(a) of the Right to Information Act, references were however made to *Rajya Sabha Unstarred Question No. 1598* and *Lok Sabha Unstarred Question No. 3207*, which revealed the following additional information:

46 http://www.thehindu.com/news/national/indias-surveillance-project-may-be-as-lethal-as-prism/article4834619.ece, accessed on Feruary 5, 2014
47 Supra. 45
48 Ibid.

• The CMS project was approved by the Cabinet Committee on Security in a meeting held on 16th July 2011.

• The interception and monitoring of any target under CMS can be done only after following the due process of law as stipulated in Section 5(2) of the Indian Telegraph Act read with Rule 419A of the Indian Telegraph Rules.

• CMS has an inbuilt mechanism of checks and balances, wherein the LEAs are unable to provision the targets themselves, and the provisioning authority is unable to see the content of the intercepted communication. Further, there is a provision of auto generation of audit trail of command logs related to interception and monitoring.

• The total fund allocation for CMS project is Rs. 400 crores. As on 12th December 2012, the expenditure incurred on R&D was Rs. 76.86 crores and on roll out of project, Rs. 4.25 crores.

• The development work of the system is largely completed. A pilot project was completed by 30th September 2011 at Delhi under which C-DOT installed two ISF servers – one each for Mahanagar Telephone Nigam Ltd. (MTNL) and Tata Communications Ltd. (TCL). The interception services were integrated and tested successfully for said service providers. Further, the system has been installed and integrated in Delhi License Service Area connecting six telecom service providers and one in Haryana License Service Area. The CMS has also been integrated with mobile number portability operators pan-India. Equipment was ordered for installation of CMS in six more Licensed Service Areas as on 12th December 2012.

However, while the interception process under the CMS is claimed to be governed by the procedure laid down by Section 5 of the Indian Telegraph Act read with Rule 419A of the Indian Telegraph Rules, the fact that the CMS is capable of Direct Electronic Provisioning of target numbers runs foul of said procedure since it dispenses with the chain of command involving manual elements such as nodal officers meant to authorize interception requests. Though this automation is said to better protect the privacy of citizens in terms of a reduction in the number of people in the know of whose/what communications are being monitored, it leaves no external non-governmental parties to verify the authenticity of interception requests. This undeniably makes clandestine/unauthorized surveillance by those so inclined a very real possibility.

4.3 Network Traffic Analysis

Though there have been earlier reports indicating its existence, the NETRA internet surveillance system [developed by Centre for Artificial Intelligence and Robotics (CAIR), a lab under Defence Research and Development Organization

(DRDO)[49]] was brought under the spotlight in earnest as recently as January 2014, when several Indian newspapers ran reports on its plans to monitor internet traffic for the use of words such as 'attack', 'bomb', 'blast' or 'kill' in tweets, status updates, emails or blogs. Since the Government has yet to make any public declarations on even the existence of NETRA, information on particulars regarding the system or its operation is rather scanty. However, from the various recent news reports, it can be gathered that NETRA will essentially be a surveillance system designed specifically to monitor the nation's internet networks including voice traffic passing through software such as Skype or Google Talk, besides write-ups in tweets, status updates, emails, instant messaging transcripts, internet calls, blogs and forums.[50] Not much is known regarding how this is proposed to be done, what technology will be employed, under what authority it will operate or what procedural safeguards are in place to prevent misuse of intercepted data. NETRA being strictly an internet surveillance system, it should operate under the provisions Sections 69 and 69B of the Information Technology Act read with the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules and the Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data and Information) Rules since they collectively prescribe the legal framework for interception of internet traffic and meta-data respectively. However, said legislations contain no provisions that allow the conduct of perpetual mass surveillance, which is exactly what NETRA seemingly does. So the question of how NETRA operates in conformance with governing laws as they stand today remains unanswered and open to speculation.

NETRA will essentially be a surveillance system designed specifically to monitor the nation's internet networks.

Various news reports have also stated that an inter-ministerial group comprising officials of the Cabinet Secretariat, Home Ministry, Defence Research and Development Organization, CAIR, Intelligence Bureau, Center for Develo-pment of Telematics and Computer Emergency Response Team that recently discussed the deployment strategy of NETRA favored allocation of 300 GB of storage space to a maximum of three security agencies, including the IB and Cabinet Secretariat, for intercepted internet traffic, with an extra 100 GB assigned to the remaining LEAs.[51] The resultant sum total of about 1 TB of storage for intercepted data would be a ridiculously minuscule amount. However, it was later clarified by an SFLC.in source with claimed direct links to the DRDO that NETRA storage servers known as 'nodes'

49 http://www.livemint.com/Politics/To4wvOZX7RmLM4VqtBshCM/India-to-deploy-Internet-spy-system-Netra.html accessed on February 12, 2014

50 Ibid.

51 http://articles.economictimes.indiatimes.com/2014-01-06/news/45918687_1_security-agencies-netra-inter-ministerial-group, accessed on February 12, 2014

will be installed at the ISP level at more than 1000 locations across India, each with a storage capacity of 300 GB. So a total of 300 TB of storage will be allocated initially. In any case, details surrounding the mysterious internet surveillance system continue to be hazy at best and one can only wait until more details emerge.

4.4 National Intelligence Grid

Conceptualized in the aftermath of the infamous 26/11 Mumbai terror attacks, NATGRID is envisioned as an ambitious counter-terrorism initiative to be undertaken on public-private partnership that will utilize technologies like Big Data and analytics to study and analyze huge amounts of data from various intelligence and enforcement agencies to help track suspects and prevent such attacks.[52]

NATGRID will utilize technologies like Big Data and analytics to study and analyze huge amounts of data from various intelligence and enforcement agencies to help track suspects and prevent such attacks.

According to a response dated 9 June, 2011 from the NATGRID Office to an RTI request filed by SFLC.in, NATGRID will be established as an attached office of the Ministry of Home Affairs, as per the decision of the Cabinet Committee on Security (full text of NATGRID's response available at http://sflc.in/unravelling-natgrid/). It will reportedly collate and analyze data generated by 21 standalone databases belonging to various agencies and ministries of the Indian Government, which includes tax and bank account details, credit card transactions, visa and immigration records and itineraries of rail and air travel.[53] It will then make this pool of data available to all security agencies — including the RAW, the IB, the ED, the National Investigation Agency, the CBI, the Directorate of Revenue Intelligence and the Narcotics Control Bureau.[54] Armed with the use of Big Data and other analytics technologies, NATGRID is also expected to facilitate robust information sharing by various LEAs, which will supposedly strengthen their ability to detect terrorist activity, and swiftly piece together information that could help pre-empt attacks or find the perpetrators in the unfortunate event.[55] To this end, in the budget of 2012-2013, the NATGRID was allotted funds to the tune of Rs. 364.80 crore, which was revised to just Rs. 10.99 crore due to non clearance for some of the plans by the Government. However, it witnessed a quantum jump in the 2013-2014 budget getting a six-fold increase with an allocation of Rs. 66.5 crore. The NATGRID is said to have been in partial operation since January 2013[56].[57]

52 http://www.business-standard.com/article/current-affairs/natgrid-to-use-big-data-analytics-to-track-suspects-113122900191_1.html, accessed on February 18, 2014
53 http://www.thehindu.com/news/national/article3529461.ece , accessed on February 18, 2014
54 Ibid.
55 http://pib.nic.in/newsite/erelease.aspx?relid=102034 , accessed on February 18, 2014
56 http://www.moneycontrol.com/news/current-affairs/natgrid-to-be-operational-by-jan-2013_555474.html , accessed on February 18, 2014
57 http://articles.economictimes.indiatimes.com/2013-12-22/news/45475848_1_natgrid-national-intelligence-grid-raman, accessed on February 18, 2014

Again, not much is known regarding the specifics of NATGRID, its governing laws or other procedural safeguards to prevent the leak or misuse of collated data that is clearly of a highly sensitive nature. Responding to the previously mentioned RTI request, the PMO further offered that all possible measures are being taken to prevent misuse of NATGRID, though the specific measures were refused to be disclosed 'for security reasons'. Interestingly, soon after a series of follow-up RTI requests , NATGRID was added to Schedule II of the RTI Act, which contains a list of Government instrumentalities excluded from the purview of the Act. Resultantly, concerned Public Information Officers are no longer obliged to entertain RTI requests relating to NATGRID and all subsequent requests have been categorically denied claiming this exemption.

In any case, NATGRID CEO Raghu Raman argues that rather than promoting invasion into people's privacy, NATGRID will protect all information and act as a deterrent to misuse of data, though the 'how' of it was left unaddressed. As per the initial plan, the user agencies will route their queries through NATGRID, which will function as a central facilitation centre, to data sources such as banks and airlines. These agencies will also get bolted-down computer terminals for accessing information from NATGRID.[58] However, bolted-down terminals are far from adequate protection against misuse of sensitive data and in the absence of any additional public statements on safeguard mechanisms within NATGRID, one is left at the all-too-familiar situation of depending on the user agencies' goodwill to prevent misuse of the sensitive personal data of citizens.

4.5 Unlawful interception and monitoring

Apart from the above-mentioned surveillance systems, whose existence at least are publicly known and whose operations may shakily be argued as legitimate in the eyes of law, there is reason to believe that the authorities also indulge in discreet communications surveillance practices, the legality of which are questionable at best. Please be mindful of the fact that this information is unverified.

For instance, SFLC.in was informed by a delegate at a recent conference that he manages a company that 'helps the Government track down terrorists'. What is truly disturbing about this ostensibly noble endeavour is the manner in which said 'terrorists' are tracked down. In the delegate's own words, his team of experts are given a list of individuals suspected of having links to terrorist organizations by various LEAs such as the CBI, based on which they proceed to infiltrate the targets' electronic communications including e-mail and chats through the use of trojans or other malicious software. Such software disguised as .jpg attachments among others, are injected into target systems by agents often assuming false identities that are determined to hold interest to the targets based on their age groups and other available

58 http://articles.economictimes.indiatimes.com/2011-06-12/news/29647514_1_natgrid-warsaw-data, accessed on February 18, 2014

information. Once the software is successfully injected, they proceed to secure access to personal data such as e-mail and IM IDs and passwords, which are used to log in to the corresponding user accounts and scan the contained communications histories for evidence of terrorist links. Any evidence so found is accordingly handed to the requisitioning LEAs that will then use said evidence in their own internal investigation processes. The delegate further indicated that his company is only one of several others engaged in a similar business model in India.

If true, the legality of operations of such private surveillance companies is entirely questionable in view of the fact that the Information Technology Act expressly criminalizes the infiltration and discreet retrieval of information of the nature discussed above. Additionally, the discreet nature of these endeavours means there is no public accountability or oversight involved whatsoever. This also brings up the rather unsettling question of what other discreet surveillance mechanisms are currently in deployment that we haven't had the fortune of coming to know of through chance encounters.

5. Privacy: The Indian Perspective

Having seen the many surveillance programs that keep a close watch on India's communication networks, one cannot help but ask the following question: what is the Indian take on a Right to Privacy?

On the outset, a Constitutional Right to Privacy is conspicuous only in its absence. However, this is not to say there hasn't been considerable debate in judicial and legislative circles on the matter.

> A seven-judge bench of the Supreme Court held that Article 21 of the Constitution of India contains an implicit right to privacy.

In the case of Kharak Singh v. The State of UP & Ors.[59], two judges of a seven-judge bench of the Supreme Court held that Article 21 of the Constitution of India, which guarantees citizens a Fundamental Right to Life and Personal Liberty, contains an implicit right to privacy. The same was held in Govind v. State of Madhya Pradesh[60] as well as R R Gopal & Anr. v. State of Tamil Nadu[61]. While the aforementioned cases examined a physical violation of privacy, in a more recent case of People's Union for Civil Liberties v. Union of India & Anr.[62], a two-judge bench of the Supreme Court examined the Constitutionality of Section 5(2) of the Indian Telegraph Act and came to the conclusion that the right to hold a telephone conversation in the privacy of one's home or office without interference can certainly be claimed as right to privacy. The judgement further said that telephone-tapping, unless conducted in accordance with procedure established by law, violates Articles 19(1)(a) and 21 of the Constitution. It also reiterated that while the right to privacy, by itself, has not been identified under the Constitution, it is still a part of the Right to Life and Personal Liberty enshrined under Article 21.

Thus, the judicial stand on the matter of privacy is clear, in that it recognizes right to privacy as an implicit content of Article 21, but admits that as a concept it may be too broad and moralistic to define judicially. Instead, the judiciary recommends that possible infringements of the right to privacy be examined on a case-by-case basis.

The citizens' privacy rights were once again brought under the judicial scanner in 2010, when the Supreme Court admitted a petition [*Ratan Tata v. UoI* {W.P.(C).No. 398 of 2010}] filed by renowned industrialist Ratan Tata, where Mr. Tata claimed that his right to privacy as guaranteed by Article 21 had been violated in view of the Government's failure to prevent the leakage and eventual publication of certain intercepted phone-conversations betwe-en himself and Niira Radia – a popular corporate lobbyist. He was aggrieved by the failure of the authorities to take

59 (1964) 1 SCR 332
60 (1975) 2 SCC 148
61 (1994) 6 SCC 632
62 (1997) 1 SCC 301

adequate steps to protect the privacy of those whose conversations were recorded, and to act in accordance with the Indian Telegraph Rules in dealing with these transcripts. In his petition, Mr. Tata sought directions from the Court to the effect that the authorities take all steps to retrieve the leaked recordings, and the CBI conduct a thorough inquiry into the matter. He also sought a direction to ensure that there was no further publication of these recordings. In light of the significant questions of law involved, the Supreme Court's decision in the matter is expected to significantly contribute to the existing judicial canon on right to privacy in the Indian context. Mr. Tata's petition is presently pending before the Court.

Aside from judicial pronouncements, right to privacy in India is also influenced by the Universal Declaration on Human Rights (UDHR) and International Covenant on Civil and Political Rights (ICCPR), both of which recognize the individual's right to privacy. While India is a signatory to the UDHR and ICCPR, provisions of these international documents are non-enforceable in law. However, it is almost an accepted proposition of law that the rules of customary international law which are not contrary to the municipal law shall be deemed to be incorporated in the domestic law. In addition, Article 51 of the Constitution directs that the State shall endeavour to *inter alia*, foster respect for international law and treaty obligations in the dealings of organised peoples with one another. Article 51 being a Directive Principle of State Policy, the contained direction is again non-enforceable. However, it serves as a constitutional reminder that the State's obligations under international law and treaties must not be transgressed. So in summation, India is under a non-enforceable obligation to incorporate Right to Privacy into its laws. Though non-enforceable, this obligation serves an important purpose of providing legally recognized ideals, the adoption of which every effort should be directed at. In other words, it serves as an accepted dictate that there needs to be a legislatively recognized Right to Privacy in India.

Further, a committee headed by Justice A P Shah published a report in October 2012, which dealt comprehensively with privacy laws across jurisdictions. The object of said report was to provide a set of recommendations on the right to privacy in light of expanding State and corporate surveillance capabilities in the digital age. The report identified nine National Privacy Principles that serve to establish safeguards and procedures over the collection, processing, storage, retention, access, disclosure, destruction, and anonymization of sensitive personal information, personal identifiable information, sharing, transfer, and identifiable information , along with the rights of the data subject in relation to such information:

1. *Notice at the time of collection of data, breach, access etc.:* At the time of collection, the content, use and purpose of collection must be notified to the data subject

2. *Choice and Consent*: The choice to (not) provide their personal

information must always be in the hands of the data subject

3. *Collection Limitation*: Only that data which is necessary for the object to be achieved must be sought from the data subject

4. *Purpose limitation*: The information must only be used for the purpose for which it is sought

5. *Access and Correction*: Data subjects should have access to their own information as well as the ability to correct and amend the information that is kept with the data controller

6. *Disclosure of Information*: The disclosure of personal information of the data subject shall only be given to third parties after their informed consent has been taken

7. *Security*: Reasonable security safeguards shall be put in place to ensure that unauthorized persons cannot access or destroy the data

8. *Openness*: Practices shall be implemented that ensure compliance with privacy principles

9. *Accountability*: The data controller shall be accountable for all the information that he keeps

The report aptly observes that currently, privacy protection in India is piecemeal and does not uphold these principles in a systematic function. Especially considering the entire array of surveillance systems that directly threaten the Right to Privacy of Indian citizens, an overarching Privacy Act, which specifically incorporates these principles and sets up an enforcement mechanism to ensure compliance is an immediate necessity.

While the privacy protection in India is inadequate in its current state, there have been significant dialogues in the international framework relating to a fundamental Right to Privacy in the online sphere. The next chapter accordingly looks beyond India and seeks to understand various internationally guaranteed human rights on which State surveillance would have significant bearing.

6. Surveillance and Human Rights

Articles 12 and 17 of the UDHR and ICCPR respectively guarantee a Right to Privacy.

Article 19 of both the UDHR[63] and the ICCPR[64] guarantee the people of the world a Right to Freedom of Opinion and Expression. These rights affirm that everyone has the right to hold opinions without interference, and to seek, receive and impart information and ideas of kinds through any media and regardless of frontiers. Unimpeded freedom of opinion and expression of the kind envisaged by the UDHR and ICCPR will be impossible if people must live in perpetual fear of sanction for their unpopular opinions or information, including those voiced in private fora.

Further, Articles 12 and 17 of the UDHR[65] and ICCPR[66] respectively guarantee a Right to Privacy. Privacy can be defined as the presumption that individuals should have an area of autonomous development, interaction and liberty, and a private sphere with or without interaction with others, free from State intervention and excessive unsolicited intervention by other uninvited individuals.[67] However, the lack of explicit articulation of the content of this right has led to difficulties in its application and enforcement. There remain challenges with respect to what constitutes the private sphere and in establishing notions of what constitutes public interest.

General Comment No. 16 (1988) by the Center for Civil and Political Rights (CCPR), adopted by the Human Rights Council (HRC) of the United Nations (UN) said surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations, should be prohibited. It also indicated that the gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. In its General Comment No. 34 (2011), the HRC analyzed the relationship

63 Article 19, UDHR: *Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.*

64 Article 19, ICCPR: *1. Everyone shall have the right to hold opinions without interference.*
2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart ideas and information of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.
3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary: (a) For respect of the rights or reputations of others; (b) For the protection of national security or of public order (ordre public), or of public health or morals.

65 Article 12, UDHR: *No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.*

66 Article 17, ICCPR: *1. No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation.*
2. Everyone has the right to the protection of the law against such interference or attacks.

67 Lord Lester and D. Pannick (ed.), *Human Rights Law and Practice, 1st ed. 2004, para 4.82*

between the Right to Freedom of Expression and Opinion and the Right to Privacy, underlining how the latter is often an essential requirement for the realization of the latter.

Also relevant is the Resolution on Right to Privacy in the Digital Age[68] adopted by the UN General Assembly on 19th December 2013. The Resolution, jointly drafted by Germany and Brazil, has the U.N. General Assembly call upon its members 'to review their procedures, practices and legislation regarding the surveillance of communications, their interception and collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law'. It notes that new technologies that increase the ability for surveillance, interception and data collection by governments, companies and individuals may violate or abuse human rights, in particular the right to privacy. The adoption of this Resolution is a milestone since the General Assembly has established, for the first time, that human rights should prevail irrespective of the medium and therefore need to be protected both off-line and on-line.[69] While there has been much debate over the binding force of UN General Assembly Resolutions, they are generally accepted as legally non-binding. Nevertheless, the significance of the Resolution must not be undermined since it is indicative of the consensual point-of-view of an international consortium of nations on a matter of socio-legal significance. Though this might not strictly translate into immediate structural changes across the world, it undeniably has considerable import on international dialogues on the matter of state surveillance and human rights.

Further, the UN General Assembly had, in its above-mentioned Resolution on Right to Privacy in the Digital Age, asked the UN High Commissioner on Human Rights (HCHR) to submit a report on the protection and promotion of the right to privacy in the context of domestic and extraterritorial surveillance and/or the interception of digital communications and the collection of personal data, including on a mass scale, to the Human Rights Council at its 27th session and to the General Assembly at its 69th session. An advance copy of this Report was released by the office of the HCHR on 30th June 2014. With regard to surveillance and collection of personal data, the Report concludes that practices in many States reveal a lack of adequate national legislation and/or enforcement, weak procedural safeguards, and ineffective oversight, all of which contribute to a lack of accountability for arbitrary or unlawful interference in the right to privacy. As an immediate measure, the Report suggests that States review their own national laws, policies and practices to ensure full conformity with international human rights law. Where there are shortcomings, States should take steps to address them, including through the adoption of a clear, precise, accessible, comprehensive and non-discriminatory legislative framework. Steps should also be taken to ensure

68 A/RES/68/167

69 Statement made by the Representative of Brazil on adoption of the Draft Resolution on Right to Privacy in the Digital Age

that effective and independent oversight regimes and practices are in place, with attention to the right of victims to an effective remedy.

Thus the international policy sentiments towards unregulated surveillance conducted by States is clear in that there is a general consensus on the resultant violations of the Right to Privacy as well as the Right to Freedom of Expression and Opinion. Both the UN General Assembly's Resolution on Right to Privacy in the Digital age and the report of the HCHR on surveillance and collection of personal data emphasize this fact and call for immediate review of national laws followed by implementation of remedial measures.

7. The Necessary and Proportionate Principles

By now, it should be amply clear that Government authorities and Law Enforcement Agencies have near-unqualified surveillance capabilities when it comes to India's communication networks. Upcoming surveillance systems such as the CMS and NETRA are demonstrably among the most invasive in the world – all the more so, considering how a patchwork of broadly worded laws wallow them to tap into virtually any network, often without the knowledge of even service providers themselves. Additionally, the whole process has no parliamentary or judicial oversight whatsoever, and the conspicuous absence of a justiciable Right to Privacy in Indian legal canons makes matters even worse.

To further illustrate the undesirability of this state of affairs, we now turn to a set of 13 international principles[70] that seek to provide a frame of reference towards determining the fairness of State surveillance programs. Led by Privacy International, Access and Electronic Frontier Foundation, and ratified by hundreds of signatory organizations (including SFLC.in) from across the world, these principles are the outcome of a year-long global consultation with civil society groups, industry and international experts in communications surveillance law, policy and technology. Bearing in mind that privacy is a fundamental human right central to the maintenance of democratic societies, the principles also serve as a comprehensive explanation of how existing human rights standards and international law apply to the new capabilities and risks of digital surveillance.

Without further ado, the determination of whether the State may conduct communications surveillance that interferes with protected information must be consistent with the following principles:

7.1 Legality

"*Any limitation to the right to privacy must be prescribed by law. The State must not adopt or implement a measure that interferes with the Right to Privacy in the absence of an existing publicly available legislative act, which meets a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of and can foresee its application. Given the rate of technological changes, laws that limit the Right to Privacy should be subject to periodic review by means of a participatory legislative or regulatory process.*"

Central/State Governments, their authorized agents and LEAs in India derive their authority to conduct communications surveillance from several legislative Acts and Rules in addition to the collective body of communications service licenses, as seen in chapters II and III. These include the Indian Telegraph Act 1885, Information Technology Act 2000, Rules framed under these Acts, Code of Criminal Procedure 1973 and service licenses granted by the Department of Telecommunications to communications service providers – including but not limited to the Unified Access Service

70 Available at https://en.necessaryandproportionate.org/text

License, Internet Service License and Unified License. Thus, measures that limit citizens' Right to Privacy arguably have their foundations in publicly available legislations and regulations.

However, there is a deeper underlying problem here in that citizens of India do not enjoy a justiciable and legislatively granted Right to Privacy to begin with. Right to Privacy in India is an uncertain, non-justiciable right that exists solely on the basis of its judicial interpretation as an implicit content of Right to Life as guaranteed by Article 21 of the Constitution of India.

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

7.2 Legitimate aim

"*Laws should only permit communications surveillance by specified State authorities to achieve a legitimate aim that corresponds to a predominantly important legal interest that is necessary in a democratic society. Any measure must not be applied in a manner which discriminates on the basis of race, color, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.*"

The crux of the principle of legitimate aim is that communications surveillance should be undertaken only towards achieving a 'predominantly important legal interest that is necessary in a democratic society'. This rightly narrows down the scope of invasive surveillance mechanisms to the most dire circumstances, where the very foundations of democratic society are at stake. With the bar set so high, surveillance cannot be undertaken on shaky grounds and in the interest of trifling ends.

An examination of the surveillance-enabling provisions found across Indian legislations will reveal that communications surveillance is currently permitted on a wide variety of broadly worded grounds, and this includes everything from protection of national security to prevention of spread of computer viruses. These validating grounds cover a ridiculous number of situations and have such sweeping ambit that legitimacy of aim is all but lost, since they effectively allow unrestricted communications surveillance to be conducted on anyone at any time.

The principle of legitimate aim therefore does not find compliance in India's communications surveillance regime.

7.3 Necessity

"*Laws permitting communications surveillance by the State must limit surveillance to that which is strictly and demonstrably necessary to achieve a legitimate aim. Communications surveillance must only be conducted when it is the only means of achieving a legitimate aim, or, when there are multiple means, it is the means least likely to infringe upon human rights. The onus of establishing this justification, in judicial as well as in legislative processes, is on the State.*"

Drawing upon the preceding principle, the principle of necessity states that communications surveillance may be conducted only when it is the least intrusive means of attaining the legitimate aim. Once again, the threshold of justifiability of surveillance is rightly set very high

Strictly speaking, Rule 419A(3) of the Indian Telegraph Rules 1951 and Rule 8 of the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009 do stipulate that 'other reasonable means' must be considered and exhausted before issuing an interception or monitoring order under the Rules. However, these cautionary provisions are purely procedural hurdles to the actual retrieval of intercepted information. Considering that around 7500 - 9000 phone-interception orders were issued by the Central Government every month (as revealed by an RTI request filed by SFLC.in), careful consideration of less intrusive alternatives in each case would be physically impossible. Further, surveillance systems such as NETRA, which *perpetually* monitor communication networks call into question the whole premise of Rules 419A and 8, since continuous availability of intercepted data would have the effect of dispensing with the very need to resort to other less intrusive means. Also, in the absence of independent oversight, there is no obligation to justify this choice of means. Thus, despite compliant legislative provisions, the principle of necessity sees questionable compliance at best in the bigger picture.

7.4 Adequacy

"*Any instance of communications surveillance authorised by law must be appropriate to fulfil the specific legitimate aim identified.*"

The principle of adequacy states that the choice of specific means of communications surveillance must correspond to the legitimate aim at hand. In other words, the mere existence of a legitimate aim must not be grounds for indulging in all kinds of communications surveillance, but the best suited form of surveillance must be identified and employed based on the surrounding circumstances.

However, as already seen, communications surveillance in India is not always conducted in pursuance of a legitimate aim for want of less intrusive alternatives. The nation's communication networks are effectively under perpetual surveillance, with the retrieval of collected information being conditional on the LEAs' procurement of a lawful order to do so. Also considering the sheer volume of such lawful orders issued, a case-by-case determination of whether surveillance is

the best alternative under the circumstances is almost certainly never done. In the face of such perpetual and unrestricted surveillance, compliance with the principles of legality, necessity or adequacy looks uncertain.

7.5 Proportionality

"*Communications surveillance should be regarded as a highly intrusive act that interferes with the rights to privacy and freedom of opinion and expression, threatening the foundations of a democratic society. Decisions about communications surveillance must be made by weighing the benefit sought to be achieved against the harm that would be caused to the individual's rights and to other competing interests, and should involve a consideration of the sensitivity of the information and the severity of the infringement on the right to privacy.*

Specifically, this requires that, if a State seeks access to or use of protected information obtained through communications surveillance in the context of a criminal investigation, it must establish to the competent, independent, and impartial judicial authority that:

> *• There is a high degree of probability that a serious crime has been or will be committed;*
>
> *• Evidence of such a crime would be obtained by accessing the protected information sought;*
>
> *• Other available less invasive investigative techniques have been exhausted;*
>
> *• Information accessed will be confined to that reasonably relevant to the crime alleged and any excess information collected will be promptly destroyed or returned; and*
>
> *• Information is accessed only by the specified authority and used for the purpose for which authorization was given.*

If the State seeks access to protected information through communication surveillance for a purpose that will not place a person at risk of criminal prosecution, investigation, discrimination or infringement of human rights, the State must establish to an independent, impartial, and competent authority:

> *• Other available less invasive investigative techniques have been considered;*
>
> *• Information accessed will be confined to what is reasonably relevant and any excess information collected will be promptly destroyed or returned to the impacted individual; and*
>
> *• Information is accessed only by the specified authority and used for the purpose for which was authorization was given.*"

This principle essentially states that the benefits of communications surveillance should always outweigh its costs i.e. surveillance should be only be resorted to following extensive contemplation of the benefits sought to be derived in contrast with the costs associated in the form of compromise of privacy. As much should

also be demonstrated before a competent, independent and impartial authority and only once this is done should the actual surveillance commence.

As already explained, this is hardly the currently practised model of communications surveillance in India. Surveillance is allowed for a number of broadly worded grounds, several of which do not qualify as legitimate aims, there isn't sufficient weighing of benefits against costs and there is no requirement to demonstrate the necessity of conducting surveillance before a judicial authority. Further, certain surveillance systems such as NETRA seemingly conduct *perpetual mass surveillance*, affording no opportunities for cost-benefit-analyses in specific instances. It would appear that communications surveillance is mostly undertaken because it is the easiest available alternative, as opposed to the least intrusive.

7.6 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:*

> 1. *Separate from the authorities conducting communications surveillance;*
>
> 2. *Conversant in issues related to and competent to make judicial decisions about the legality of communications surveillance, the technologies used and human rights; and*
>
> 3. *Have adequate resources in exercising the functions assigned to them.*"

This principle is *prima facie* violated by India's communications surveillance framework for the simple reason that there is absolutely no judicial intervention at any stage of the surveillance process. No provisions of law as they currently stand talk about judicial oversight in any capacity. An observation on the matter was also made by the Supreme Court in the case of PUCL v. UoI,[71] where judicial oversight of phone interception was held as unsustainable in the lack of express legal provisions that provide for such oversight.

Though the Indian Telegraph Rules and the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules provide for the establishment of a Review Committee towards reviewing surveillance directives, this Committee is comprised solely of members of the executive. When provisions of law stipulate systematic review of any activity capable of causing harm in the absence of oversight, it logically follows that fairness of review cannot be guaranteed in the presence of conflicting interests. If those undertaking and reviewing such potentially harmful activity belong to the same broad vehicle of the Government, conflicting interests are all but unavoidable and this leads to a complete breakdown of the review process itself.

As per the governing Acts and Rules, an order authorizing communications surveillance may be issued by the

71 (1997) 1 SCC 301

'competent authority' i.e. the Secretary in the Ministry of Home Affairs/Secretary in charge of the Home Department; actual surveillance is carried out mostly by authorized LEAs; and the Review Committee consists of the Cabinet/Chief Secretary along with Secretaries in charge of legal affairs and telecommunications. In other words, every aspect of India's surveillance regime is handled by the executive arm of the Government with no judicial intervention whatsoever and therefore, just and fair review of surveillance process is nearly impossible. Thus, the principle of competent judicial authority stands violated in its entirety.

7.7 Due process

"*Due process requires that States respect and guarantee individuals' human rights by ensuring that lawful procedures that govern any interference with human rights are properly enumerated in law, consistently practiced, and available to the general public. Specifically, in the determination on his or her human rights, everyone is entitled to a fair and public hearing within a reasonable time by an independent, competent and impartial tribunal established by law, except in cases of emergency when there is imminent risk of danger to human life. In such instances, retroactive authorization must be sought within a reasonably practicable time period. Mere risk of flight or destruction of evidence shall never be considered as sufficient to justify retroactive authorization.*"

As previously mentioned, Indian communications surveillance is technically founded in publicly available law. However, there are no means of determining the extent to and rigor with which these laws are observed in practice, since all of India's communications surveillance is conducted within an extremely closed environment with no transparency or independent oversight. The concerned enabling Acts and Rules always stipulate the observance of strict confidentiality in the surveillance process, thereby significantly limiting the amount of information on surveillance practices that is available to the general public. Government authorities routinely assure citizens that surveillance is conducted only in accordance with law, yet this claim is questionable. For instance, despite consistent assurances that the CMS operates strictly in accordance with the procedures laid down by Rule 419A of the Indian Telegraph Rules, its capability for Direct Electronic Provisioning, i.e. automated instantaneous interception without involvement of service providers, runs foul of this procedure. Similarly, there are no provisions of law that provide for the conduct of mass surveillance of any kind, yet exactly this what NETRA seemingly does when it scans the nation's internet traffic for trigger words and phrases.

Thus while publicly available law does enumerate procedures that govern interference with human rights, its consistent practice remains questionable. And even though legal remedies are available with respect to violation of rights, the efficacy of these remedies is somewhat compromised in the face of emphatic claims of legal compliance accompanied by the inability to verify these claims.

7.8 User notification

"*Individuals should be notified of a decision authorizing communications surveillance with enough time and information to enable them to appeal the decision, and should have access to the materials presented in support of the application for authorization. Delay in notification is only justified in the following circumstances:*

> 1. *Notification would seriously jeopardize the purpose for which the surveillance is authorised, or there is an imminent risk of danger to human life; or*
>
> 2. *Authorization to delay notification is granted by the competent judicial authority at the time that authorization for surveillance is granted; and*
>
> 3. *The individual affected is notified as soon as the risk is lifted or within a reasonably practicable time period, whichever is sooner, and in any event by the time the communications surveillance has been completed. The obligation to give notice rests with the State, but in the event the State fails to give notice, communications service providers shall be free to notify individuals of the communications surveillance, voluntarily or upon request.*"

There currently exist no provisions of law whereby users are notified when their communications are subjected to surveillance, and no distinction is made between situations where such notification would defeat the purpose of surveillance and otherwise. By extension, users also lack the ability to appeal the decision to surveille their communications. Even once active surveillance has been concluded, collected information is retained for specified periods after which they are destroyed – all without intimating the user. Thus it is entirely possible in the present scenario for the bulk of a users' communications to be subjected to extensive surveillance leaving him/her none the wiser.

7.9 Transparency

"*States should be transparent about the use and scope of communications surveillance techniques and powers. They should publish, at a minimum, aggregate information on the number of requests approved and rejected, a disaggregation of the requests by service provider and by investigation type and purpose. States should provide individuals with sufficient information to enable them to fully comprehend the scope, nature and application of the laws permitting communications surveillance. States should enable service providers to publish the procedures they apply when dealing with State communications surveillance, adhere to those procedures, and publish records of State communications surveillance.*"

The principle of transparency is *prima facie* violated by Indian communications surveillance. Government authorities and LEAs view communications surveillance as an exclusive State concern in which non-governmental parties have no business interfering. This is evident in the fact that surveillance systems such as the CMS and NETRA are sanctioned by high-level ministerial committees without

adequate parliamentary dialogue. The CMS in particular, while commencing initial operations, had only a partial in-principle approval from the Cabinet Committee on Security. Even questions raised by Members of Parliament on such matters are answered in such a way that as little information is divulged as possible. Save a few rare press releases, little to no information is publicly shared regarding surveillance initiatives and even purely procedural information such as internal guidelines requested under the Right to Information Act is consistently denied claiming exemption under Section 8(1)(a) as they relate to national security matters. With most of the information on State surveillance initiatives coming from investigative reports by various non-state parties, the resulting picture is a patchwork of verified data, unverified rumors and wild speculations, all of which significantly contribute to the confusion surrounding India's communications surveillance regime.

7.10 Public oversight

"*States should establish independent oversight mechanisms to ensure transparency and accountability of communications surveillance. Oversight mechanisms should have the authority to access all potentially relevant information about State actions, including, where appropriate, access to secret or classified information; to assess whether the State is making legitimate use of its lawful capabilities; to evaluate whether the State has been transparently and accurately publishing information about the use and scope of communications surveillance techniques and powers; and to publish periodic reports and other information relevant to communications surveillance. Independent oversight mechanisms should be established in addition to any oversight already provided through another branch of government.*"

Once again, all oversight of Indian communications surveillance is carried out by a single Review Committee constituted under Rule 419A of the Indian Telegraph Rules, which comprises entirely of members of the executive. This severely compromises its independence and impartiality due to the apparent conflict of interest that arises when the authorization, conduct and review of communications surveillance is carried out by a singular arm of the Government machinery. Additionally, the Committee's scope of review is restricted to the sustainability of specific interception directives issued by the concerned authorities, and does not extend to the mode of interception or subsequent use of intercepted information.

Thus the only oversight of Indian communications surveillance is of an executive nature, and has very limited scope. The public oversight principle is therefore not complied with.

7.11 Integrity of communications and systems

"*In order to ensure the integrity, security and privacy of communications systems, and in recognition of the fact that compromising security for State purposes almost always compromises security more generally, States should not compel service providers or hardware or software vendors to build surveillance or monitoring capability into their systems, or to collect or retain particular*

information purely for State surveillance purposes. A priori data retention or collection should never be required of service providers. Individuals have the right to express themselves anonymously; States should therefore refrain from compelling the identification of users as a precondition for service provision."

Thus the fundamental concern of this principle is the security of communication networks and systems. Towards securing said networks and systems, it is recommended that:

> • There should be no compulsion on vendors/service providers to facilitate surveillance
>
> • User identification must not be a precondition for service provision

Regarding the facilitation of surveillance, service licenses place Indian communications service providers under the express obligation to install surveillance equipment into their networks as and when required by the Government 'in the interest of security'. Apart from the threat of license revocation on failure to comply, surveillance-enabling provisions of law such as those found under the Indian Telegraph Act or Information Technology Act further strengthen this compulsion by prescribing penalties on the failure to provide information when called upon to do so. In addition, service providers are prohibited by service licenses from employing bulk encryption in their networks, and even when non-bulk, anything higher than a 40-bit encryption requires express approval from the Department of Telecommunications. This ban on encryption beyond 40-bits extends to individuals, groups and organizations as well. All these undeniably compromise the general security of communications networks by facilitating not only surveillance initiatives, but also malicious and targeted attacks from non-state parties.

Further, user identification is always a prerequisite for provision of communications service. Citizens are required to provide valid identification when procuring new telephone or internet connections and even when using cyber cafes for internet access. Communications service providers are also required to maintain regularly updated lists of all subscribers and make them available to authorized Government agencies. This indicates that the Government is intolerant of anonymity in the telecommunication or internet circles, and wish to be able to trace specific instances of communication to their respective points of origin.

In short, the above measures have the cumulative effect of doing exactly what the principle of integrity seeks to avoid i.e. compromising the general security of communications, as well as disallowing user anonymity in all communication spheres.

7.12 Safeguards for international cooperation

"*In response to changes in the flows of*

information, and in communications technologies and services, States may need to seek assistance from a foreign service provider. Accordingly, the mutual legal assistance treaties (MLAT) and other agreements entered into by States should ensure that, where the laws of more than one state could apply to communications surveillance, the available standard with the higher level of protection for individuals is applied. Where States seek assistance for law enforcement purposes, the principle of dual criminality should be applied. States may not use mutual legal assistance processes and foreign requests for protected information to circumvent domestic legal restrictions on communications surveillance. Mutual legal assistance processes and other agreements should be clearly documented, publicly available, and subject to guarantees of procedural fairness."

This principle essentially says that MLATs and other international agreements should not present opportunities to conduct invasive communications surveillance that would normally be disallowed in the domestic context. India currently has subsisting MLATs with 35 nations including USA, UK, Canada, France and Russia, but there are no explicit references to communications surveillance in any of said MLATs. Instead, they contain provisions that allow the request of information and evidence, surrounding which strict confidentiality must be maintained and measures implemented to prevent unauthorized access or misuse. However, this does not provide for the application of highest available standards of individual protection since there is no weighing of options involved. MLATs and other international agreements as they currently stand do not deal with communications surveillance in sufficient detail and hence the intricacies involved in international cooperation in the realm of communications surveillance still need to be worked out.

7.13 Safeguards against illegitimate access

"*States should enact legislation criminalizing illegal communications surveillance by public or private actors. The law should provide sufficient and significant civil and criminal penalties, protections for whistle blowers, and avenues for redress by affected individuals. Laws should stipulate that any information obtained in a manner that is inconsistent with these principles is inadmissible as evidence in any proceeding, as is any evidence derivative of such information. States should also enact laws providing that, after material obtained through communications surveillance has been used for the purpose for which information was given, the material must be destroyed or returned to the individual.*"

The following provisions of law deal with unauthorized access of communications:

- Section 24 read with Section 23 of the Indian Telegraph Act punishes any person, who attempts to unlawfully learn the contents of communications, with imprisonment up to one year and fine up to Rs. 500. However, the circumstances inviting penalty are limited in scope as they require the offender to physically enter Government premises or obstruct Government officials while attempting to unlawfully learn the

contents of communications.

• Section 26 of the Indian Telegraph Act punishes Government officials, who intercept, detain or disclose the content of communications without authorization, with imprisonment up to three years and fine.

• Section 43 of the Information Technology Act states that any person, who accesses and tampers with electronic devices, their content, or networks without authorization from their owner/ person-in-charge, is liable to compensate the owner/person-in-charge for damages up to Rs. 1 crore.

• Section 72 of the Information Technology Act punishes any person, who discloses information that was lawfully accessed by him/her, with imprisonment up to two years and fine up to Rs. 2 lakhs.
The above provisions of law visibly penalize illegitimate communications surveillance by both public and private actors. Also, both the Indian Telegraph Act and the Information Technology Act stipulate the destruction of all surveillance- related documents within specified periods once active surveillance has been concluded.

However, since a majority of these collective principles are not conformed to in Indian conduct of communications surveillance to begin with, the inadmissibility of information collected through non-conformant surveillance as evidence does not arise. Nor does the law tackle the admissibility of information collected in violation of its own mandates. Thus, the principle of safeguards against illegitimate access can be considered only partially observed in India.

In summation, it is seen that Indian communications surveillance is conducted in violation of most of the international principles discussed in this chapter. The principles of legitimate aim, proportionality, competent judicial authority, user notification, transparency, public oversight, and integrity of communications and systems stand entirely violated. Even the remaining principles i.e. legality, necessity and due process see only partial/questionable compliance. This clearly indicates that Indian communications surveillance is conducted in a manner that is far from what may be considered just . Of the discussed contraventions of principles, lack of a legislatively granted Right to Privacy, lack of judicial oversight and lack of transparency in surveillance require immediate and undivided attention from the law-makers since these shortcomings have the potential to translate into significant damage to the citizens of India, all the more so in the face of intrusive surveillance systems that are steadily escalating in their scale of operations.

8. Conclusion

Over the course of this report, we have seen that the GoI and its agents are authorized under various statutes and license agreements to surveil India's telephone and Internet networks on a large number of broadly worded grounds ranging from protection of national security to preventing the spread of computer viruses. Pursuant to authority so derived, several state surveillance programs already keep a close tab on our communication networks, and far more potent surveillance technologies are in the pipeline in varying stages of deployment. While the Government swears that it limits itself to targeted surveillance and does not indulge in mass surveillance of any kind, the large scale data-mining and profiling capabilities of upcoming surveillance systems such as the CMS and NATGRID are reason enough to be skeptical of this stance. Also causing concern among citizens is the fact that communications surveillance continues to be the exclusive domain of the Executive arm of the Government, which insists on keeping the public in the dark. There are no provisions for public or judicial oversight of the surveillance process and in such a scenario, one cannot help but be wary of abuse of power. To top it all off, a legislatively recognized right to privacy is conspicuously absent from Indian legal canons. Protection accorded by law to the citizens' right to privacy ends with a judicial interpretation of the right as an implicit content of right to life as guaranteed by the Constitution of India.

In the wake of the global uproar caused by Edward Snowden's revelations on US surveillance, and the sudden spike in interest around the topic of surveillance and privacy, the time has come for a comprehensive review of Indian legislative provisions that sanction and regulate our surveillance process. In this regard, the language of the law needs to be considerably narrowed down to specify objectively verifiable situations under which surveillance may be legitimately undertaken. The procedure to be followed while surveilling communications must be clearly spelled out in its entirety, and any opportunity for misuse of authority must be done away with by holding the concerned agents of intercepting agencies to the highest standards of accountability. Provision for independent oversight of the surveillance process is an immediate necessity, and the regime of blanket denial of surveillance-related information requests made by the public must be done away with. The surveillance regime in its current state needs to be made more transparent, and public trust in this regard must be rebuilt, which will not happen without a greater degree of public participation. Finally, citizens must have a legislatively recognized right to privacy, the violation of which will entitle them to constitutional remedies.

All of the above remedies are easily envisioned, but their implementation will undoubtedly present several challenges – both foreseen and unforeseen. Nothing short of a collective, concentrated effort on the part of all stakeholders in the surveillance regime, including but not limited to the Government, industry, civil society and the general public, will serve to transform India's surveillance state from its current state of opacity to one of transparency, trust and efficiency.

Appendix

The Information Technology Act, 2000

Section 28 - Power to investigate contraventions.

(1) The Controller or any officer authorised by him in this behalf shall take up for investigation any contravention of the provisions of this Act, rules or regulations made thereunder.
(2) The Controller or any officer authorised by him in this behalf shall exercise the like powers which are conferred on Income-tax authorities under Chapter XIII of the Income-tax Act, 1961 and shall exercise such powers, subject to such limitations laid down under that Act.

Section 29 - Access to computers and data.

(1) Without prejudice to the provisions of sub-section (1) of section 69, the Controller or any person authorised by him shall, if he has reasonable cause to suspect that any contravention of the provisions of this Act, rules or regulations made thereunder has been committed, have access to any computer system, any apparatus, data or any other material connected with such system, for the purpose of searching or causing a search to be made for obtaining any information or data contained in or available to such computer system.

(2) For the purposes of sub-section (1), the Controller or any person authorised by him may, by order, direct any person in-charge of, or otherwise concerned with the operation of, the computer system, data apparatus or material, to provide him with such reasonable technical and other assistance as he may consider necessary.

Section 43 - Penalty for damage to computer, computer system, etc.

If any person without permission of the owner or any other person who is in-charge of a computer, computer system or computer network, —

(a) accesses or secures access to such computer, computer system or computer network;

(b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

(c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

(d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;

(e) disrupts or causes disruption of any computer, computer system or computer network;

(f) denies or causes the denial of access to

any person authorised to access any computer, computer system or computer network by any means;

(g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder;

(h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network, he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.
Explanation.—For the purposes of this section,—

(i) "computer contaminant" means any set of computer instructions that are designed—

(a) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or

(b) by any means to usurp the normal operation of the computer, computer system, or computer network;

(ii) "computer data base" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;

(iii) "computer virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the perfor-mance of a computer resource or attaches itself to another computer resource and operates when a progr-amme, data or instruction is executed or some other event takes place in that computer resource;

(iv) "damage" means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.

Section 69 – Power 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 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 the incitement to the commission of any cognizable offence relating to the above or for the investigation of any offence, it may, subject to the provisions of sub-section

(2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be

intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource.

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

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

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

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

(c) provide information stored in computer resource

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

Section 69B - Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security.

(1) The Central Government may, to enhance Cyber Security and for identification, analysis and prevention of any intrusion or spread of computer contaminant in the country, by notification in the official Gazette, authorize any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource.

(2) The Intermediary or any person in-charge of the Computer resource shall when called upon by the agency which has been authorized under sub-section (1), provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating, transmitting, receiving or storing such traffic data or information.

(3) The procedure and safeguards for monitoring and collecting traffic data or information, shall be such as may be prescribed.

(4) Any intermediary who intentionally or knowingly contravenes the provisions of subsection (2) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

Explanation: For the purposes of this section,

(i) "Computer Contaminant" shall have the meaning assigned to it in section 43

(ii) "traffic data" means any data identifying or purporting to identify any person, computer

system or computer network or location to or from which the communication is or may be transmitted and includes communications origin, destination, route, time, date, size, duration or type of underlying service or any other information.

Section 72 - Penalty for breach of confidentiality and privacy.

Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Indian Telegraph Act, 1885

Section 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.

Section 3(1AA) - Definitions

'telegraph' means any appliance, instrument, material or apparatus used pr capable of use for transmission or reception of signs, signals, writing, images

and sounds or intelligence of any nature by wire, visual or other electro- magnetic emissions, radio waves or Herizan waves, galvanic, electronic or magnetic means.

Explanation- 'Radio waves' or 'hertizan waves' means electro- magnetic waves of frequencies lower than 3,000 giga-cycles per second propagated in space without artificial guide.

Section 23 - Intrusion into signal-room, trespass in telegraph office or obstruction

If any person--

a) without permission of competent authority, enters a signal-room of a telegraph office of the Government, or of a person licensed under this Act, or

b) enters a fenced enclosure round such a telegraph office in contravention of any rule or notice not to do so, or

c) refuses to quit such room or enclosure on being requested to do so by any officer or servant employed therein, or

d) wilfully obstructs or impedes any such officer or servant in the performance of his duty, he shall be punished with fine which may extend to five hundred rupees.

Section 24 - Unlawfully attempting to learn the contents of messages

If any person does any of the acts mentioned in Section 23 with the intention of unlawfully learning the contents of any message, or of committing any offence punishable under this Act, he may (in addition to the fine with which he is punishable under Section 23) be punished with imprisonment for a term which may extend to one year.

Section 26 - Telegraph officer or other official making away with or altering, or unlawfully intercepting or disclosing messages, or divulging purport of signals.

If any telegraph officer, or any person, not being a telegraph officer, but having official duties connected with any office which is used as a telegraph office—

(a) wilfully, secrets, makes away with or alters any message which he has received for transmission or delivery, or

(b) wilfully, and otherwise than in obedience to an order of the Central Government or of a State Government, or of an officer specially authorised [by the Central or a State Government] to make the order, omits to transmit, or intercepts or detains, any message or any part thereof, or otherwise than in pursuance of his official duty or in obedience to the direction of a competent Court, discloses the contents or any part of the contents of any message, to any person not entitled to receive the same, or

(c) divulges the purport of any telegraphic signal to any person not entitled to become acquainted with the same,he shall be punished with imprisonment for a term which may extend to three years, or with fine, or with both.

Indian Telegraph Rules, 1951

Rule 419-A

(1) Directions for interception of any message or class of messages under sub-section (2) of Section 5 of the Indian Telegraph Act, 1885 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.

The Information Technology (Intermediaries Guidelines) Rules, 2011

Rule 3(7) - Due diligence to be observed by intermediary

When required by lawful order, the intermediary shall provide information or any such assistance to Government Agencies who are lawfully authorised for investigative, protective, cyber security activity. The information or any such assistance shall be provided for the purpose of verification of identity, or for prevention, detection, investigation, prosecution, cyber security incidents and punishment of offences under any law for the time being in force, on a request in writing staling clearly the purpose of seeking such information or any such assistance.

Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

Rule 6-Disclosure of information.

(1) Disclosure of sensitive personal data or information by body corporate to any third party shall require prior permission from the provider of such information, who has provided such information under lawful contract or otherwise, unless such disclosure has been agreed to in the contract between the body corporate and provider of information, or where the disclosure is necessary for compliance of a legal obligation:

Provided that the information shall be shared, without obtaining prior consent from provider of information, with Government agencies mandated under the law to obtain information including sensitive personal data or information for the purpose of verification of identity, or for prevention, detection, investigation including cyber incidents, prosecution, and punishment of offences. The Government agency shall send a request in writing to the body corporate possessing the sensitive personal data or information stating clearly the purpose of seeking such information. The Government agency shall also state that the information so obtained shall not be published or shared with any other person.

(2) Notwithstanding anything contain in sub-rule (1), any sensitive personal data on Information shall be disclosed to any third party by an order under the law for the time being in force.

Information Technology (Guidelines for Cyber Cafe) Rules, 2011

Rule 7 - Inspection of Cyber Cafe

(1) An officer, not below the rank of Police Inspector as authorised by the licensing agency, is authorized to check or inspect cyber café and the computer resource or network established therein at any time for the compliance of these rules. The cyber café owner shall provide every related document, registers and any necessary information to the inspecting officer on demand.

Code of Criminal Procedure

Section 91 - Summons to produce document or other thing.

(1) Whenever any Court or any officer in charge of a police station considers that the production of any document or other thing is necessary or desirable for the purposes of any investigation, inquiry, trial or other proceeding under this Code by or before such Court or officer, such Court may issue a summons, or such officer a written order, to the person in whose possession or power such document or thing is believed to be, requiring him to attend and produce it, or to produce it, at the time and place stated in the summons or order.

(2) Any person required under this section merely to produce a document or other thing shall be deemed to have complied with the requisition if he causes such document or thing to be produced instead of attending personally to produce the same.

(3) Nothing in this section shall be deemed -

(a) to affect, sections 123 and 124 of the Indian Evidence Act, 1872 (1 of 1872), or the Bankers, Books Evidence Act, 1891(13 of 1891), or

(b) to apply to a letter, postcard, telegram or other document or any parcel or thing in the custody of the postal or telegraph authority.

Notes

ABOUT SFLC.IN

SFLC.IN is a donor supported legal services organization that brings together lawyers, policy analysts, technologists, and students to protect freedom in the digital world. We promote innovation and open access to knowledge by helping developers make great Free and Open Source Software, protect privacy and civil liberties of citizens in the digital world through education and provision of pro bono legal advice, and help policy makers make informed and just decisions with the use and adoption of technology. Please feel free to contact us to learn more about protecting your rights in the online world.

K-9, Birbal Road, Second Floor,
Jangpura Extension
New Delhi-110014, India
Tel: +91-11-43587126
Fax: +91-11-24320809
www.sflc.in

WORLD WIDE WEB FOUNDATION

With support from

World Wide Web Foundation's Web We Want Initiative

The World Wide Web Foundation was established in 2009 by Web inventor Sir Tim Berners-Lee to tackle the fundamental obstacles to realizing his vision of an open Web available, usable, and valuable for everyone. Their global initiative "Web We Want " is a global movement to defend, claim and change the future of the Web. The campaign is responding to threats to the future of the Web with a practical and positive vision — unleashing the power of people from around the world to defend, claim and change a Web that is for everyone. We aim to bring about real change at a national and global level. "