Security, Surveillance and Data Sharing Schemes and Bodies in India

- **By Maria Xynou and Elonnai Hickok**

Following the 2008 Mumbai terrorist attacks, India had implemented a wide range of data sharing and surveillance schemes. Though developed under different governments the purpose of these schemes has been to increase public safety and security by tackling crime and terrorism. As such, two data sharing schemes have been proposed - the National Intelligence Grid (NATGRID) and the Crime and Criminal Tracking Network & Systems (CCTNS), as well as several surveillance systems, such as the Lawful Intercept and Monitoring (LIM) system, the Network Traffic Analysis system (NETRA), state Internet Monitoring Systems and the Central Monitoring System (CMS). This chapter details the various schemes and provides policy recommendations for their improvement, with regards to the protection of the right to privacy and other human rights.

National Intelligence Grid (NATGRID)

The National Intelligence Grid (NATGRID) is a proposed as an integrated intelligence grid that will link the databases of several departments and ministries of the Government of India in order to collect comprehensive patterns of intelligence that can be readily accessed by intelligence agencies. NATGRID is considered to be a data linking and mining project and the initial stage would have involved the "real-time linking" of data between various agencies.[1] The Ministry of Home Affairs first proposed the creation of NATGRID following the Mumbai 2008 terrorist attacks and stated the following:

"Today, each database stands alone. It does not talk to another database. Nor can the 'owner' of one database access another database. As a result, crucial information that rests in one database is not available to another agency. In order to remedy the deficiency, the Central Government has decided to set up NATGRID. Under NATGRID, 21 sets of databases will be networked to achieve quick, seamless and secure access to desired information for intelligence/enforcement agencies. This project is likely to be completed in 18 – 24 months from now." [2]

In the aftermath of the Mumbai terrorist attacks, NATGRID was set up by the Government at an estimated cost of Rs. 4,000 – 5,000 crore to enable the monitoring of terrorist operations

[1] Aman Sharma, *"NATGRID to get running in 4 months"*, The Economic Times, 07 December 2013, http://articles.economictimes.indiatimes.com/2013-12-07/news/44909645_1_databases-national-counter-terrorism-centre-information-security

[2] Government of India, Ministry of Home Affairs, Press Information Bureau, *"Home Minister proposes radical restructuring of security architecture"*, 23 December 2009, http://www.pib.nic.in/newsite/erelease.aspx?relid=56395

through existing banking, finance and transportation networks[3]. NATGRID is an attached office of the Ministry of Home Affairs and has been conceived to develop a framework to enhance India's counter-terror capabilities. In order to achieve this, NATGRID engaged with the National Institute of Smart Government (NISG) to provide manpower. As such, NISG invited professionals from the fields of technology and management to work with NATGRID as consultants[4].

The Ministry of Home Affairs had sought over Rs. 3,400 crore for its high-tech intelligence network, NATGRID, which aims to collect sensitive information from databases of departments like the police, banks, tax and telecom to track any terror suspect and incident. The Cabinet Committee on Security has already approved NATGRID, which aims to bring together police and security agencies for a real-time exchange of data across the country[5].

The Ministry of Home Affairs had also announced that it will issue an executive order to give a legal framework to NATGRID that will give 11 security agencies real-time access to 21 citizen data sources to track terror activities. Such an executive order was needed since the various ministries and departments, otherwise called "provider agencies", would have needed a legal mandate to link and share their data sources in real-time through NATGRID with the 11 intelligence and investigative agencies, termed as user agencies. These citizen data sources include bank account details, telephone records, passport data and vehicle registration details, among other types of data[6].

Raghu Raman, the then CEO of NATGRID, had stated:

"In many ways it (NATGRID) has started. There are certain elements being helped out where it is required...[...]...NATGRID has been delayed to make sure that the security protocols of the data sources it is using are very strong...[...]...The security (of NATGRID) has been kept at the highest level. As a matter of fact, I can technology-wise guarantee you that the way NATGRID will protect data will be far higher than the protection given to the data in its original location...[...]...NATGRID is a tool in background. It is assisting agencies. It is only a pointer, like a compass. It is like Google. When you search for anything on Google it points you to go here and go there...Likewise it (NATGRID) enables an officer to very quickly get a 360-degree view of a situation..."[7]

It was further reported that NATGRID will utilize analytics to process the huge volumes of data generated from the 21 data sources so as to analyse events, match patterns and track suspects. Data mining appears to be at the core of NATGRID, which aims to create comprehensive patterns of intelligence by linking the 21 data sources and analysing them[8]. To

[3] NT Balanarayan, *"NATGRID Partial Roll Out Very Soon"*, Medianama, 17 January 2014, http://www.medianama.com/2014/01/223-natgrid-partial-roll-out/

[4] Government of India, Ministry of Home Affairs, *National Intelligence Grid,* 30 May 2013, http://www.davp.nic.in/WriteReadData/ADS/eng_19138_1_1314b.pdf

[5] Deccan Herald, *"MHA seeks over Rs. 3,400 crore for NATGRID"*, 29 January 2014, http://www.deccanherald.com/content/181065/mha-seeks-over-rs-3400.html

[6] Aman Sharma, *"NATGRID to get legal powers soon"*, The Economic Times, 10 September 2013, http://articles.economictimes.indiatimes.com/2013-09-10/news/41938113_1_executive-order-national-intelligence-grid-databases

[7] DNA India, *"NATGRID begins operations; high security protocols deployed"*, 22 December 2013, http://www.dnaindia.com/india/report-natgrid-begins-operations-high-security-protocols-deployed-1939160

[8] Press Trust of India, *"NATGRID to use Big Data & analytics to track suspects"*, The Business Standard, 29 December 2013, http://www.business-standard.com/article/current-affairs/natgrid-to-use-big-data-analytics-

facilitate an early roll out, the Ministry of Home Affairs had allowed its databases, the National Population Register (NPR) and the Immigration, Visa, Foreigners Registration and Tracking System (IVFRT), to be linked to NATGRID[9].

Crime and Criminal Tracking Network & Systems (CCTNS)

Following the 2008 Mumbai terrorist attacks, the creation of the Crime and Criminal Tracking Network & Systems (CCTNS) was proposed. In particular, the Union Home Minister mentioned the role of the CCTNS during the IB Endowment lecture at Vigyan Bhawan, New Delhi on 23rd December 2009 in the following words:

"The police stations in the country are, today, virtually unconnected islands. Thanks to telephones and wireless, and especially thanks to mobile telephones, there is voice connectivity between the police station and senior police officers, but that is about all. There is no system of data storage, data sharing and accessing data. There is no system under which one police station can talk to another directly. There is no record of crimes or criminals that can be accessed by a Station House Officer, except the manual records relating to that police station. Realising the gross deficiency in connectivity, the Central government is implementing an ambitious scheme called "Crime and Criminal Tracking Network System (CCTNS)".[10]

As such, the goals of the CCTNS are to facilitate the collection, storage, retrieval, analysis, transfer and sharing of data and information at the police stations and between the police stations and the State Headquarters and the Central Police Organisations[11]. The Cabinet Committee on Economic Affairs approved the CCTNS in 2009 within the outlay of Rs. 2,000 crore in the 11th Five Year Plan. This project was initiated by the Ministry of Home Affairs and implemented by the National Crime Records Bureau[12].

The CCTNS was formally launched in early January 2013 in New Delhi. This project aims to create a comprehensive and integrated system for effective policing and sharing data of crimes and criminals among 14,000 police stations across all the 35 states and Union Territories of India[13]. The CCTNS is part of the process of modernising the police force and was introduced under the national e-governance scheme. In its first phase in Tamil Nadu in February 2012, the CCTNS was introduced in Thiruvallur, Ariyalur, Sivaganga and Coimbatore, where the First Information Reports and details of the cases have been computerised and stored at the State Informatics Centre[14].

to-track-suspects-113122900191_1.html

[9] ET Bureau, *"NATGRID to take off soon on home ministry data"*, The Economic Times, 17 January 2014, http://articles.economictimes.indiatimes.com/2014-01-17/news/46301449_1_natgrid-the-national-intelligence-grid-home-ministry

[10] Sh. P Chidambaram, Ex-Union Home Minister, *"Ex-Union Home Minister's mission statement for NCRB under CCTNS"*, Crime and Criminal Tracking Network & System (CCTNS), National Crime Records Bureau, Ministry of Home Affairs, http://ncrb.nic.in/cctns.htm

[11] Ibid

[12] Government of India, Press Information Bureau, Cabinet Committee on Economic Affairs, *"Crime and Criminal Tracking Network & Systems (CCTNS) project"*, 2009, http://pib.nic.in/newsite/erelease.aspx?relid=49261

[13] The Hindu, *"Govt launches crime tracking pilot project"*, 04 January 2013, http://www.thehindu.com/news/national/govt-launches-crime-tracking-pilot-project/article4272857.ece

[14] Delta Bureau, *"Crime Tracking Easier with CCTNS"*, The Hindu, Tamil Nadu, 18 September 2013,

It is estimated that Rs. 2,000 crore have been allocated for the CCTNS, which connects more than 21,000 locations[15]. Under the CCTNS project, approximately 14,000 police stations throughout India are being automated and connected, excluding 6,000 police offices which are high in the police hierarchy. The objectives of the CCTNS project are the following[16]:

- Increase transparency by automating the function of police stations
- Improve the delivery of citizen-centric services through the effective usage of ICT
- Provide the Investigating Officers of the Civil Police with tools, technology and information to facilitate the investigation of crime and detection of criminals
- Improve the function of the police in various other areas, such as Law and Order, Traffic Management, etc.
- Facilitate the interaction and sharing of information among police stations, districts, State/UT headquarters and other police agencies
- Assist Senior Police Officers in the better management of the Police Force
- Keep track of the progress of cases (including those in Court)
- Reduce the manual and redundant keeping of records[17]

Home Secretary R.K. Singh stated that the CCTNS will provide a comprehensive database of crimes and criminals, which will enable law enforcement agencies in tracking down criminals moving from one place to another. Mr. Singh also stated that the CCTNS will increase transparency in police administration, since individuals will be able to launch complaints online and to view the status of their reports. Moreover, Mr. Singh stated:

"This will be a wide database. It will help in arresting criminals and investigating any case. This will be a big milestone."[18]

Additionally, the Minister of State for Home R.P.N. Singh stated that the CCTNS will create a nation-wide environment for real-time sharing of crime and criminal information. Referring to the gang-rape of a girl in Delhi, Singh said:

"We could not protect this one daughter of India but now we have to protect the over a billion men and women for whom we are responsible. This is the greatest service we can do for our country."[19]

Data Sharing Centres and Bodies

- **The National Cyber Coordination Centre:** The Central Government is currently in the process of approving a new security body that would be responsible for cyber intelligence and cyber security. According to news items, the body will come under the National Information Board[20] and would be a multi- agency body under the

http://www.thehindu.com/news/national/tamil-nadu/crime-tracking-easier-with-cctns/article5141371.ece

[15] The Hindu, *"Govt launches crime tracking pilot project"*, 04 January 2013, http://www.thehindu.com/news/national/govt-launches-crime-tracking-pilot-project/article4272857.ece

[16] Government of India, National Crime Records Bureau, *"About CCTNS"*, http://ncrb.nic.in/AboutCCTNS.htm

[17] Ibid

[18] The Hindu, *"Govt launches crime tracking pilot project"*, 04 January 2013, http://www.thehindu.com/news/national/govt-launches-crime-tracking-pilot-project/article4272857.ece

[19] Ibid

[20] http://www.hindustantimes.com/india-news/cyber-protection-body-pushes-ahead/article1-1174753.aspx

Department of Electronics and IT.[21] The NCCC is currently a Rs. 950 crore project with the objective of streamlining coordination between intelligence agencies and to screen all forms of meta data.[22] The NCCC will also monitor internet traffic within the country and coming in and out of the country at the international gateways for cyber threats.[23] Mandates that are currently beyond the scope of India's CERT-IN.

- **The Forensics Science Laboratories:** Under the Information Technology Act Forensic Science Laboratories are 'Examiners of Electronic Evidence' for the purpose of providing expert opinion on digital evidence. Divisions within Forensic Science Laboratories include: physics, chemistry, biology, serology, ballistics, documents, finger prints, forensic psychology, photo, computer forensic science & scientific aids divisions with laboratories for computer forensics and DNA profiling which are ISO/IEC 17025 compliant.[24] Forensic Science Laboratories are under the administrative control of the CBI and answer to the Ministry of Home Affairs. Experts from the CFSL can also give expert opinion, testify, and provide evidence in a court of law.
- **New Delhi Police – Centre for analysing social media:** As of June 2014 the New Delhi Police are reported to be in the process of establishing a centre to monitor social media content for the purpose of understanding the 'mood' of the public and to identify potential threats or worrisome content.[25] The centre is supposed to run on its own dedicated server with software approved by the government. In news items, officials have noted that, though not as complex, the centre is meant to be like the monitoring centre set up by the London police after riots that took place in 2011.[26]
- **The National Counter Terrorism Centre (NCTC):** In 2012 the NCTC was proposed as a centralized body under the Unlawful Activities (Prevention) Act, 1967, for the purpose of addressing and deploying counter terrorism measures of the Union and state governments.[27] Though the NCTC was supported by the Central Government, many State Governments opposed its establishment citing concerns around lack of consensus amongst states and effectiveness of the centre.[28] The Home Ministry justified the need for a centralized counter terrorism centre that specifically had jurisdiction over state governments because of the lack of action by states, a lack of professionalism, and the use of state forces for political purposes.[29] It was proposed to locate the NCTC under the umbrella of the Intelligence Bureau, with the Director of the NCTC being the Additional Director of the IB. The stated purpose of the NCTC was to analyse and maintain relevant intelligence and develop and direct responses to the Union and State government in the face of terror threats. Additionally, the NCTC was to maintain a data base of terrorists and their associates, friends, families, supporters, and all other information pertaining to terrorists.[30] In an

[21] http://currentaffairs.gktoday.in/fact-box-national-cyber-coordination-centre-nccc-0620136970.html

[22] http://www.hindustantimes.com/india-news/rs-950-crore-centre-to-shield-india-from-cyber-attacks-proposed/article1-1252849.aspx

[23] http://currentaffairs.gktoday.in/fact-box-national-cyber-coordination-centre-nccc-0620136970.html

[24] http://cbi.nic.in/cfsl/about.htm

[25] http://www.indiatvnews.com/news/india/delhi-police-social-media-content-centre-to-analyze-content-37816.html

[26] http://www.bgr.in/news/delhi-police-to-set-up-centre-to-analyze-social-media-posts/

[27] http://www.satp.org/satporgtp/countries/india/document/papers/2012/NCTC_2012.pdf

[28] http://indianexpress.com/article/news-archive/latest-news/narendra-modi-slams-nctc-new-draft-says-upa-will-misuse-it-to-target-opposition/

[29] http://www.ipcs.org/pdf_file/issue/IB181-Chari-NCTC.pdf

[30] http://www.satp.org/satporgtp/countries/india/document/papers/2012/NCTC_2012.pdf

order titled "The National Counter Terrorism Centre (Organisation, Functions, Powers, and Duties Order, 2010" it was highlighted that the NCTC should not replicate the efforts of other agencies in the country, and instead should 'work through' them. To enable this, the order recommended that NCTC staff should be drawn from RAW, JIC, NTRO, DIA, DGMI, DAI, CEIB, CBDT, CBEC etc. The Order also noted that Officers in the 'Operations' division will have the power to search and arrest as per section 43A of the Unlawful Activities (Prevention) Act, 1967, the NCTC will also have the power to set up Inter-State Intelligence Support Teams and to use the services of the National Security Guard and other special forces, and seek information such as documents, reports, transcripts, and cyber information from other agencies. A Standing Council to ensure that the NCTC in the single and effective point of control and coordination for counter terrorism measures.[31]

- **Safe City Project and Fusion Data Centres:** In 2013 the Ministry of Home Affairs, PM Division published guidelines for the development of mega policing projects. It is envisioned that Delhi, Kolkata, Mumbai, Chennia, Hyderabad, Bangalore, and Ahemadabad would implement the Mega City Policing projects. Among other aspects, the guidelines provide instructions for the establishment of Fusion Cenres/Data Centres. According to the guidelines: "*The Fusion/Data Centre would be playing a very crucial role in prevention and detection as also investigation of crime or security related challenges. It will, however be necessary to have upto date and comprehensive databases from various fields, for example, Vehicle registration numbers, Unique ID numbers of the citizens, residential addresses, Pan card details, crime related details. The accessibility of these databases by the Fusion Centres will have to be ensured by defining MoU or Law Enforcement Agreements or State Legislations to enable the State to have access to the private data on individuals without any encroachment on the privacy rights of the individuals*."[32]

In 2010 66.92 crores were dedicated to revamping special branches/intelligence agencies. This included GIS mapping, integrated documentation systems and integrated data centres, voice loggers, IED Jammers, VHF Mobile Jammers.[33] These funds are sanctioned by the High Powered Committee under the MHA.

Lawful Intercept & Monitoring (LIM) Systems

In September 2013 it was reported that the Indian Government was running Lawful Intercept and Monitoring (LIM) systems over the last years, widely in secret. Following the Mumbai 2008 terrorist attacks, the Centre for Development of Telematics (C-DOT) deployed the LIM systems for the monitoring of Internet traffic, emails, web browsing, Skype and any other Internet activity of users in India[34].

In particular, mobile operators in India have deployed their own LIM systems to monitor communications running through their networks, which allow for the "lawful interception" of calls by government agencies. Such "lawful interception" is carried out under Section 5(2) of the Indian Telegraph Act, 1885, read with Rule 419(A). In the case of Internet traffic, the LIM

[31] http://www.satp.org/satporgtp/countries/india/document/papers/2012/NCTC_2012.pdf

[32] http://mha.nic.in/sites/upload_files/mha/files/SafeCity-150313.pdf

[33] http://mha.nic.in/sites/upload_files/mha/files/Scheme-MPF-11Nov.pdf

[34] Shalini Singh, *"Govt. Violates Privacy Safeguards to Secretly Monitor Internet Traffic"*, The Hindu, 08 September 2013, http://www.thehindu.com/news/national/govt-violates-privacy-safeguards-to-secretly-monitor-internet-traffic/article5107682.ece

systems are deployed by the Government of India at the international gateways of large Internet Service Providers (ISPs). As such, the functioning of the LIM systems is beyond the control of these ISPs and these surveillance systems are completely controlled by the Government[35].

Lawful interception by mobile operators using LIM systems appears to entail targeted The In 2013 the Government of India proposed Standard Operating Procedures (SOPs) for phone-tapping in the country[36]. According to news items reporting on these guidelines:

"The purpose of the Standard Operating Procedures (SOPs) is to lay minimum required guidelines for lawful interception and monitoring process across all telecom service providers (TSPs) to ensure systematic and tamper-proof monitoring of target numbers and have uniformity on critical issues of interception and monitoring which should be followed scrupulously."[37]

All requests for interception and monitoring of voice, SMS, GPRS, VAS, MMS, video calls or VoIP can be made under the Indian Telegraph Act, 1885. These Standard Operating Procedures provide guidelines for all interception and monitoring of telecommunications, which is carried out under the Indian Telegraph Act, 1885, or under the Information Technology (Amendment) Act, 2008. As such, mobile operators in India which use LIM systems for the lawful interception of their communications may have to comply with the Standard Operating Procedures issued by the Government[38].

In the case of Internet traffic though, the Government's monitoring systems appear to have the capability to carry out mass surveillance, since they are installed between the ISPs Internet Edge Router (PE) and the core network and have an "always live" link to the entire traffic. As such, LIM systems appear to have broad surveillance capabilities with access to all Internet activity, which is not limited to IPs, email addresses, URLs or webmails, but which expand to a broad search across all Internet traffic using "keywords" and "keyphrases"[39].

LIM systems are available to nine security agencies, including the Intelligence Bureau (IB), the Research and Analysis Wing (RAW) and the Ministry of Home Affairs (MHA)[40]. Other agencies which are authorised for lawful interception include the Central Board of Direct Taxes (CBDT), the Central Bureau of Investigation (CBI), the Directorate of Revenue Intelligence (DRI) and the Narcotics Control Bureau (NCB)[41].

In early 2012 the Government of India issued Standard Operating Procedures (SOPs) for lawful interception and monitoring. The Standard Operating Procedures provide guidelines to security agencies based on which the lawful interception and monitoring of communications

[35] Ibid

[36] DNA India, *"Government issues standard operating procedures for phone-tapping in India"*, 10 January 2014, http://www.dnaindia.com/india/report-government-issues-standard-operating-procedures-for-phone-tapping-in-india-1948730

[37] Ibid

[38] Ibid

[39] Shalini Singh, *"Govt. Violates Privacy Safeguards to Secretly Monitor Internet Traffic"*, The Hindu, 08 September 2013,http://www.thehindu.com/news/national/govt-violates-privacy-safeguards-to-secretly-monitor-internet-traffic/article5107682.ece

[40] Ibid

[41] Ritu Sarin, *"Govt sets norms for lawful interception and monitoring"*, The Indian Express, 17 February 2012, http://archive.indianexpress.com/news/govt-sets-norms-for-lawful-interception-and-monitoring/913034/0

should be carried out. These guidelines state, among other things, that the interception of communications should not exceed 180 days and that orders for interception should be issued in emergency situations[42]. It remains unclear, though, if the LIM systems used by the Government at the international gateways of ISPs are in compliance with the Standard Operating Procedures.

Additionally, it was reported in July 2013 that BlackBerry granted the Indian Government access to its messaging services, which include BlackBerry Messenger (BBM) and BlackBerry Internet Service (BIS) email. BlackBerry though emphasized that the Government of India will not have access to the BlackBerry Enterprise Server (BES). Through the lawful interception system for BlackBerry services, the Indian authorities will be able to track email and email attachments sent over the consumer-version of BlackBerry Internet Service (BIS), to see when chats sent over BlackBerry Messenger (BBM) were delivered and read and to monitor which websites were visited[43]. BlackBerry has issued a statement confirming its cooperation with the Indian Government and has stated the following:

"The lawful access capability now available to BlackBerry's carrier partners meets the standard required by the Government of India for all consumer messaging services offered in the Indian marketplace."[44]

Network Traffic Analysis (NETRA) System

In 2013 it was reported by the media that the Indian Government was soon launch a Network Traffic Analysis (NETRA) system, which will possibly be capable of real-time detection of suspicious "keywords" and "keyphrases" in social media, emails, blogs, tweets, instant messaging services, and in other types of Internet content[45]. It has also been reported that the Ministry of Home Affairs is finalising the NETRA system, which will also likely be capable of capturing any dubious voice traffic through online communications[46]. This system is possibly going to be carried out with the purpose of tackling crime and terrorism in India.

The NETRA system has been developed by the Centre for Artificial Intelligence and Robotics (CAIR), a lab under the Defence Research and Development Organisation (DRDO). The deployment strategy of NETRA was recently discussed between an inter-ministerial group comprising of officials of the Cabinet Secretariat, Home Ministry, DRDO, CAIR, Intelligence Bureau, Centre for Development of Telematics (C-DOT) and Computer Emergency Response Team (CERT-In). Along with the discussion on NETRA's deployment strategy, this inter-ministerial group also discussed a strategy on how to deal with computer security incidents, track system vulnerabilities and promote effective IT security practices across India[47]. As

[42] Ritu Sarin, *"Govt sets norms for lawful interception and monitoring"*, The Indian Express, 17 February 2012, http://archive.indianexpress.com/news/govt-sets-norms-for-lawful-interception-and-monitoring/913034/0

[43] BBC News Technology, *"India is 'ready to use' BlackBerry message intercept system"*, 11 July 2013, http://www.bbc.co.uk/news/technology-23265091

[44] Ibid

[45] Vikas SN, *"Indian Government Plans Internet Monitoring System Netra"*, Medianama, 06 January 2014, http://www.medianama.com/2014/01/223-indian-govt-internet-monitoring-system-netra/

[46] PTI, *"Govt to launch internet spy system 'Netra' soon"*, The Times of India, 06 January 2014, http://articles.timesofindia.indiatimes.com/2014-01-06/internet/45917976_1_security-agencies-netra-cabinet-secretariat

[47] PTI, *"India to deploy Internet spy system 'Netra'"*, Livemint & The Wall Street Journal, 06 January 2014,

quoted in news items, a government official stated:

"When NETRA is operationalised, security agencies will get a big handle on monitoring activities of dubious people and organisations which use the Internet to carry out nefarious designs."[48]

Central Monitoring System (CMS)

In 2009, following the Mumbai 2008 terrorist attacks, the Government of India envisioned the creation of a Central Monitoring System (CMS) which would centralise the interception of communications data and enable access to it by law enforcement agencies. As such, the Central Monitoring System started off as a project run by the Centre for Communications Security Research and Monitoring (CCSRM), along with the Telecom Testing and Security Certification (TTSC) project[49].

The Central Monitoring System (CMS), which was largely covered by the media in 2013, was actually approved by the Cabinet Committee on Security (CCS) on 16th June 2011 and the pilot project was completed by 30th September 2011. Ever since, the CMS has been operated by India's Telecom Enforcement Resource and Monitoring (TERM) cells, and has been implemented by the Centre for Development of Telematics (C-DOT), which is an Indian Government owned telecommunications technology development centre. The CMS has been implemented in three phases, each one taking about 13-14 months[50]. Government funding of the CMS has reached at least Rs. 450 crore (around USD 72 million)[51].

Prior to the CMS, all service providers in India were required to have Lawful Interception Systems installed at their premises in order to carry out targeted surveillance of individuals by monitoring communications running through their networks[52]. As per amendments to service providers licenses, all Telecom Service Providers (TSPs) in India are required to integrate Interception Store & Forward (ISF) servers with their pre-existing Lawful Interception Systems. Once ISF servers are installed in the premises of TSPs in India and integrated with Lawful Interception Systems (LIM), they are then connected to the Regional Monitoring Centres (RMC) of the CMS. Each Regional Monitoring Centre (RMC) in India is connected to the Central Monitoring System (CMS). In short, the CMS involves the collection and storage of data intercepted by TSPs in central and regional databases[53].

http://www.livemint.com/Politics/To4wvOZX7RmLM4VqtBshCM/India-to-deploy-Internet-spy-system-Netra.html

[48] PTI, *"Indian government to launch internet spy system 'Netra' soon"*, DNA India, 05 January 2014, http://www.dnaindia.com/scitech/report-indian-government-to-launch-internet-spy-system-netra-soon-1945867

[49] Maria Xynou, *"India's Central Monitoring System (CMS): Something to Worry About?"*, The Centre for Internet and Society (CIS), 30 January 2014, http://cis-india.org/internet-governance/blog/india-central-monitoring-system-something-to-worry-about

[50] Ibid

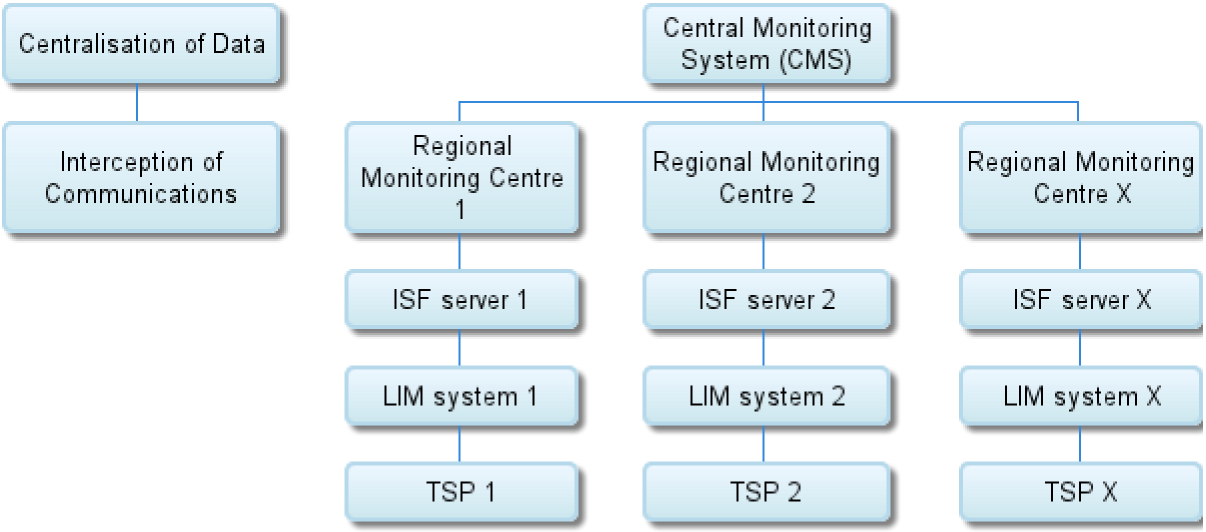
[51] CIOL Bureau, *"Government's Central Monitoring System to be operational soon"*, 11 March 2013, http://www.ciol.com/ciol/news/184770/governments-central-monitoring-system-operational-soon

[52] Shalini Singh, *"Govt. Violates privacy safeguards to secretly monitor Internet traffic"*, The Hindu, 09 September 2013, http://www.thehindu.com/news/national/govt-violates-privacy-safeguards-to-secretly-monitor-internet-traffic/article5107682.ece

[53] Maria Xynou, *"India's Central Monitoring System (CMS): Something to Worry About?"*, The Centre for Internet and Society (CIS), 30 January 2014, http://cis-india.org/internet-governance/blog/india-central-

In other words, all data intercepted by TSPs is automatically transmitted to Regional Monitoring Centres, and subsequently automatically transmitted to the Central Monitoring System. This means that the CMS authority will have centralized access to intercepted data. This is due to the fact that, unlike in the case of the current lawful interception regime where the nodal officers of TSPs are notified about interception requests, the CMS allows for data to be automatically transmitted to its data centre, without the involvement of TSPs[54].

The above is illustrated in the following chart:



Centralisation of Data
Interception of Communications
Central Monitoring System (CMS)
Regional Monitoring Centre 1
Regional Monitoring Centre 2
Regional Monitoring Centre X
ISF server 1
ISF server 2
ISF server X
LIM system 1
LIM system 2
LIM system X
TSP 1
TSP 2
TSP X

The CMS, if implemented, will be connected with the Telephone Call Interception System (TCIS) which will help monitor voice calls, SMS and MMS, fax communications on landlines, CDMA, video calls, GSM and 3G networks[55]. Such surveillance will likely expand to Internet communications through mobile phones, but it remains unclear if Internet Service Providers (ISPs) will be connected to the central and regional databases of the CMS. Without any manual intervention from TSPs, the CMS will be equipped with Direct Electronic Provisioning, filters and alerts on the target numbers[56]. Call Details Records (CDR) analysis and data mining could also be used through the CMS to assist law enforcement agencies in identifying the personal information of target numbers[57].

monitoring-system-something-to-worry-about

[54] Centre for Internet and Society, *Brief Material for Honourable MOC & IT Press Briefing on 16.07.2013*, http://cis-india.org/internet-governance/blog/new-cms-doc-2

[55] Maria Xynou, *“India's 'Big Brother': The Central Monitoring System (CMS)”*, The Centre for Internet and Society (CIS), 08 April 2013, http://cis-india.org/internet-governance/blog/indias-big-brother-the-central-monitoring-system

[56] Deepa Kurup, *“In the dark about 'India's PRISM'”*, The Hindu, 16 June 2013, http://www.thehindu.com/sci-tech/technology/in-the-dark-about-indias-prism/article4817903.ece

[57] Maria Xynou, *“India's 'Big Brother': The Central Monitoring System (CMS)”*, The Centre for Internet and Society (CIS), 08 April 2013, http://cis-india.org/internet-governance/blog/indias-big-brother-the-central-

The interface testing of TSPs and their Lawful Interception Systems has already been completed and, as of June 2013, 70 ISF servers have been purchased for six License Service Areas and are being integrated with the Lawful Interception Systems of TSPs. The Centre for Development of Telematics has already fully installed and integrated two ISF servers in the premises of two of India's largest service providers: MTNL and Tata Communications Limited. In Delhi, ISF servers which connect with the CMS have been installed for all TSPs and testing has been completed. In Haryana, three ISF servers have already been installed in the premises of TSPs and the rest of currently being installed. In Chennai, five ISF servers have been installed so far, while in Karnataka, ISF servers are currently being integrated with the Lawful Interception Systems of the TSPs in the region[58].

The Centre for Development of Telematics plans to integrate ISF servers which connect with the CMS in the premises of service providers in the following regions[59]:

- Delhi
- Maharashtra
- Kolkata
- Uttar Pradesh (West)
- Andhra Pradesh
- Uttar Pradesh (East)
- Kerala
- Gujarat
- Madhya Pradesh
- Punjab
- Haryana

In order to require Telecom Service Providers (TSPs) to intercept all telecommunications in India as part of the CMS, clause 41.10 of the Unified Access Services (UAS) License Agreement was amended in June 2013[60]. In particular, the amended clause includes the following:

"But, in case of Centralized Monitoring System (CMS), Licensee shall provide the connectivity up to the nearest point of presence of MPLS (Multi Protocol Label Switching) network of the CMS at its own cost in the form of dark fibre with redundancy. If dark fibre connectivity is not readily available, the connectivity may be extended in the form of 10 Mbps bandwidth upgradeable up to 45 Mbps or higher as conveyed by the Government, till such time the dark fibre connectivity is established. However, LICENSEE shall endeavor to establish connectivity by dark optical fibre at the earliest. From the point of presence of

monitoring-system

[58] Maria Xynou, *"India's Central Monitoring System (CMS): Something to Worry About?"*, The Centre for Internet and Society (CIS), 30 January 2014, http://cis-india.org/internet-governance/blog/india-central-monitoring-system-something-to-worry-about

[59] Ibid

[60] Government of India, Ministry of Communications and IT, Department of Telecommunications, *"Amendment to the UAS License Agreement regarding Central Monitoring System"*, June 2013, http://cis-india.org/internet-governance/blog/uas-license-agreement-amendment

MPLS network of CMS onwards traffic will be handled by the Government at its own cost."[61]

With regards to the UAS License Agreement that TSPs are required to comply with, amended clause 41.10 specifies certain details about how the CMS functions. In particular, the amended clause mandates that TSPs in India will provide connectivity up to the nearest point of presence of MPLS (Multi Protocol Label Switching) network of the CMS at their own cost and in the form of dark optical fibre. From the MPLS network of the CMS onwards, traffic will be handled by the Government at its own cost[62]. It is noteworthy that a Memorandum of Understanding (MoU) for MPLS connectivity has been signed with one of India's largest ISPs/TSPs: BSNL. In fact, Rs. 4.8 crore have been given to BSNL for interconnecting 81 CMS locations of the following License Service Areas[63]:

- Delhi
- Mumbai
- Haryana
- Rajasthan
- Kolkata
- Karnataka
- Chennai
- Punjab

Clause 41.10 of the UAS License Agreement also mandates that the hardware and software required for monitoring calls will be engineered, provided, installed and maintained by the TSPs at their own cost. Moreover, this clause mandates that TSPs are required to monitor *at least 30 simultaneous calls* for each of the nine designated law enforcement agencies. In addition to monitored calls, clause 41.10 of the UAS License Agreement also requires service providers to make the following records available to Indian law enforcement agencies:[64]

- Called/calling party mobile/PSTN numbers
- Time/date and duration of interception
- Location of target subscribers (Cell ID & GPS)
- Data records for failed call attempts
- CDR (Call Data Records) of Roaming Subscriber
- Forwarded telephone numbers by target subscriber

Furthermore, draft Rule 419B under Section 5(2) of the Indian Telegraph Act, 1885, allows for the disclosure of "message related information" / Call Data Records (CDR) to Indian authorities[65]. Call Data Records, otherwise known as Call Detail Records, contain metadata

[61] Ibid

[62] Ibid

[63] Maria Xynou, *"India's Central Monitoring System (CMS): Something to Worry About?"*, The Centre for Internet and Society (CIS), 30 January 2014, http://cis-india.org/internet-governance/blog/india-central-monitoring-system-something-to-worry-about

[64] Government of India, Ministry of Communications and IT, Department of Telecommunications, *"Amendment to the UAS License Agreement regarding Central Monitoring System"*, June 2013, http://cis-india.org/internet-governance/blog/uas-license-agreement-amendment

[65] Maria Xynou, *"India's Central Monitoring System (CMS): Something to Worry About?"*, The Centre for

(data about data) that describe a telecommunication transaction, but not the content of that transaction. In other words, Call Data Records include data such as the phone numbers of the calling and called parties, the duration of the call, the time and date of the call, and other such information, while excluding the content of what was said during such calls[66]. According to draft Rule 419B, directions for the disclosure of Call Data Records can only be issued on a national level through orders by the Secretary to the Government of India in the Ministry of Home Affairs, while on the state level, orders can only be issued by the Secretary to the State Government in charge of the Home Department.[67]

Other than this draft Rule and the amendment to clause 41.10 of the UAS License Agreement, no law exists which mandates or regulates the Central Monitoring System (CMS). This surveillance system is regulated under Section 5(2) of the Indian Telegraph Act, 1885, which empowers the Indian Government to intercept communications on the occurrence of any “public emergency” or in the interest of “public safety”, when it is deemed “necessary or expedient” to do so in the following instances:[68]

- the interests of the sovereignty and integrity of India
- the security of the State
- friendly relations with foreign states
- public order
- for preventing incitement to the commission of an offense

Interception requests from law enforcement agencies are provisioned by the CMS authority, which has access to the intercepted data by all TSPs in India and which is stored in a central database. As of June 2013, 80% of the CMS Physical Data Centre has been built so far[69]. The CMS replaces the existing manual system of interception and monitoring to an automated system, which is operated by TERM cells and implemented by the Centre for Development of Telematics[70]. Training has been imparted to the following law enforcement agencies:[71]

- Intelligence Bureau (IB)
- Central Bureau of Investigation (CBI)
- Directorate of Revenue Intelligence (DRI)

Internet and Society (CIS), 30 January 2014, http://cis-india.org/internet-governance/blog/india-central-monitoring-system-something-to-worry-about

[66] Ray Horak, *Telecommunications and Data Communications Handbook*, Wiley, 21 July 2008.

[67] Maria Xynou, *“India's Central Monitoring System (CMS): Something to Worry About?”*, The Centre for Internet and Society (CIS), 30 January 2014, http://cis-india.org/internet-governance/blog/india-central-monitoring-system-something-to-worry-about

[68] Government of India, Ministry of Communications and Information Technology, Department of Telecommunications, *The Indian Telegraph Act, 1885,* http://www.ijlt.in/pdffiles/Indian-Telegraph-Act-1885.pdf

[69] Maria Xynou, *“India's Central Monitoring System (CMS): Something to Worry About?”*, The Centre for Internet and Society (CIS), 30 January 2014, http://cis-india.org/internet-governance/blog/india-central-monitoring-system-something-to-worry-about

[70] Deepa Kurup, *“In the dark about 'India's PRISM'”*, The Hindu, 16 June 2013, http://www.thehindu.com/sci-tech/technology/in-the-dark-about-indias-prism/article4817903.ece

[71] Maria Xynou, *“India's Central Monitoring System (CMS): Something to Worry About?”*, The Centre for Internet and Society (CIS), 30 January 2014, http://cis-india.org/internet-governance/blog/india-central-monitoring-system-something-to-worry-about

- Research & Analysis Wing (RAW)
- National Investigation Agency (NIA)
- Delhi Police

According to the brief material for the Honourable MOC and IT Press Briefing on 16th July 2013, the CMS will better protect the privacy of individuals and maintain their security due to the following reasons:[72]

1. The CMS will *just automate* the existing process of interception and monitoring, and all the existing safeguards will continue to exist

2. The interception and monitoring of communications will continue to be in accordance with Section 5(2) of the Indian Telegraph Act, 1885, read with Rule 419A

3. The CMS will enhance the privacy of citizens, because it will no longer be necessary to take authorisation from the nodal officer of the Telecom Service Providers (TSPs) – who comes to know whose and which phone is being intercepted

4. The CMS authority will provision the interception requests from law enforcement agencies and hence, a complete check and balance will be ensured, since the provisioning entity and the requesting entity will be different and the CMS authority will not have access to content data

5. A non-erasable command log of all provisioning activities will be maintained by the system, which can be examined anytime for misuse and which provides an additional safeguard.

[72] Centre for Internet and Society, *Brief Material for Honourable MOC & IT Press Briefing on 16.07.2013,* http://cis-india.org/internet-governance/blog/new-cms-doc-2