SURVEILLANCE OF ELECTRONIC COMMUNICATION IN INDIA: A MISBALANCE BETWEEN PRIVACY AND SECURITY

*** Namrata Choudhary**

Introduction

Surveillance means observation and collection of data to provide evidence for a purpose[1]. *Electronic Surveillance* is an advanced form of eaves dropping. Electronic surveillance employs sophisticated electronic equipment to intercept private conversations or observe conduct that is meant to be private. It includes the use of small radio transmitters or "bugs" to listen in on telephone or in-person conversations, the use of lasers to intercept conversations inside a room from the slight vibrations of the window glass, and the use of thermal imaging scopes for observing conduct inside a structure. Many of these sophisticated forms of surveillance require a search warrant because they violate a person's reasonable expectation of privacy. This area of law is in a constant state of flux as courts interpret the use of new technologies[2].

Surveillance is, for a modern nation- state *condicio sine qua non*—an essential element without which it will eventually cease to exist which has now proved to be a necessary evil. With the growing IT sector various surveillance technologies has also been introduced like internet, CCTVs, telephone and e-mail id etc.

Historical Background of Surveillance of Electronic Communication

Concept of surveillance is not at all new is being followed and practiced since ages. In 4th century BCE, Kautilya's Arthasastra recognized espionage as an institution in itself and enjoined good rulers to heed and study the information gathered from the spies. Surveillance of electronic communications helps the Government in not only furrow the law breakers but also to detect and prevent crime and adds an undue advantage in enforcement of law.

Surveillance through the mode of interception of wire communications began long before the Civil War. The inventions and use of the microphone, dictograph recorder, and hidden cameras were made to conduct surveillance by late 18th century. Post World War I surveillance played an

[1] As defined by Black's Law Dictionary 2nd Edition
[2] Definition provided by Nolo's Plain English Law dictionary

important role in Palmer raid[3] where the government rounded up as many as 6000 enemy aliens and supposed subversives on the basis of evidence procured. World War II marked business fo manufacturing of wiretapping and other form of electronic surveillance.

In India

Arthashatra is of India so surveillance is not new to it. Before British regime the Kings, emperors maintained a dynamic system of spy consisting of officials from court. These men gathered secret from among the ministers and the people of the territory and reported the happenings of other states too, in course of welfare of the king.

During British Empire, surveillance was done at a grand scale, evident from the fact that British Official beforehand were informed of independence moves made by Indians and had a record of wireless inceptions made between the social activists India and abroad.

However post independence, nation became Republic, it devoid of any such law incorporated which limited the extent of surveillance. Till today there is no express law which concerns on surveillance expressly and the access, transfer and retention of CDRs (Call Detail Records) is also weakly defined.

International concern for imbalance between Privacy and Surveillance

United Nation Organization:

United Nation (UN) has been repeatedly being asked to establish a new international charter to stop international mass scale state surveillance on individuals. The petitioners have urged the UN to create an *International Bill of Digital Rights* that will ensure protection of civil rights in the digital age and adher to proposed charter. The main aim of the bill is to "*enshrine the protection of civil rights in the internet age*.[4]"

[3] A number of attacks on Socialists and Communists in the United States which took place from 1918 to 1921.
[4]Available at http://www.theweek.co.uk/world-news/nsa/56443/worlds-top-authors-demand-un-drafts-bill-digital-rights,last visited on March 12, 2014 PM

UN General Assembly, on 18th December 2013, unanimously adopted a resolution aiming at protection of the right of privacy against unlawful surveillance in the digital age. It calls its members to respect and protect the right of privacy and to review their procedures, practices and legislation regarding the surveillance of communications, with a view to upholding the right to privacy of all their obligations under international human rights law[5].

United States

In 1967, after the key decision in the case of *Olmstead v. United States* (1928) and in *Katz v. United States (1967)* the Supreme Court made clear that eavesdropping — bugging private conversations or wiretapping phone lines — counted as a search that required a warrant.

The federal wiretapping statute commonly known as '*Title III'* or the '*Wire Tap Act*' (1968) requires police to get a warrant often termed as '*Super Warrant'* to conduct a wire tapping. Act contains enumerated offenses that is, a list of crimes —the ones that can be investigated with a wiretap order. But due to addition of numerous crimes in the past 30 years, Act seems totally ineffective. Later, *Electronic Communication Privacy Act 1986* updated the federal Wiretap Act.[6].

United Kingdom

UK is governed by provisions of *Regulation of Investigatory Powers Act, 2000* for surveillance and investigation by governmental bodies. The Act gives guidelines to public authorities such as Police or governmental departments who want to obtain any private information which can be done in case of terrorism, crime, public safety or emergency services.[7]

[5] iPolitics, Associated Press,UN unanimously approves resolution aimed at protecting privacy against unlawful surveillance, December 18th 2013, available at http://www.ipolitics.ca/2013/12/18/un-unanimously-approves-resolution-aimed-at-protecting-privacy-against-unlawful-surveillance/ last visited on march 12th 10.40 PM

[6] Available at https://it.ojp.gov/default.aspx?area=privacy&page=1285 last visited at 10.57 AM on 21st March 21, 2014

[7] Available at https://www.gov.uk/surveillance-and-counter-terrorism, last visit at 10.32 AM on 22nd March 22, 2014

Europe

In Europe, there are no direct laws provided to govern surveillance the uses of guidelines of UK's Regulation Act are followed in Europe. Recently, *European General Data Protection Regulation Act* has been introduced by the Council in Europe on seeing the development of Information Technology sector all over the world and flow of personal data within Europe.[8].

Laws governing Surveillance in India with their lackings:

Although there is no as such prescribed guideline regarding yet are many acts and rules passed by legislation which governs surveillance indirectly. Some of them are:

Section 69 *Information Technology Amendment Act, 2008* gives power to government to intercept, monitor or decrypt any data or information stored on any computer resources for the reason of public safety, public order etc. but the lacuna being, identity of authorized person is unknown. However by the virtue of the Act **CERT-In**[9] has been made but the problem being that it comes into operation on attack on Indian Computers or resources or when server's are being hacked or crashed by foreign body or person within or outside India. Thus, the law provided is inadequate.

After independence, Indian Telegraph Rules 1951 was issued and the rule 419 attempted to bring about a procedure to regulate inceptions of communications. But both where challenge and subsequently examined by the apex court in 1996[10]. In the landmark decision, the Supreme Court held that phone communications were protected by the right to privacy which flowed from the right to personal liberty. Following 1978 decision that required intrusions into personal liberty conform to a procedure that is just, fair and reasonable, the Supreme Court measured the interception provisions of the Telegraph Act against that standard and found it wanting[11].

[8]Available at http://highfieldsoffice.wordpress.com/2013/02/10/eu-new-laws-on-surveillance-and-privacy european-citizens-visitors-should-have-none-of-course-in-the-name-of-greater-common-security/ and http://en.wikipedia.org/wiki/Data_Protection_Directive, last visited at 10.37 Am on 22 March 2014

[9] CERT-In is "The India Computer Emergency Response Team" which is a government mandated IT security organization. They main task of the organization is to respond to computer security incidences, and to report vulnerabilities and promote effective IT security. Created by Indian Department of Information Technology in 2004

[10] Union for Civil Liberties (PUCL) Vs. Union of India, dated 18.12.1996 in Writ Petition (C) No.256/1991, AIR 1997 SC 568

[11] Ibid

SC also defined the word '*public emergency'* which would mean the prevailing of a sudden condition affecting the people at large, concerning the interest of public safety, sovereignty and integrity, security of State, friendly relations with sovereign States[12].

In 1999, government incorporated these procedures into a new rule 419-A of the Telegraph Rules which restricted the power to order phone-taps to only senior administrative officers. Many laws and rules have though indirectly yet supported the governmental bodies working for the purpose of surveillance but there is no such any legal framework passed by parliament in a relation to surveillance and authorities who has power to monitor and block information for any computer recourse. As per the new Rule, data collected by CMS will be accessible to governmental bodies like Intelligence Bureau, Research and Analysis Wing, Central Bureau of Investigation, National Investigation Agency[13].

But the irony being, legality of the bodies which are established exclusively for the surveillance on internet, cell phone, private messages, powers and functions of authorities, situations under which surveillance can be done etc. and security of data to be kept by them is unknown and the provisions of their established is also a question. Adding, in India the intelligence agencies and law enforcement agencies are practically governed by no law and the constitutional validity of National Investigation Agency Act, 2008 is still doubtful. Further, India lacks a constitutionally sound lawful interception law. Phone tapping in India is still done in an unconstitutional manner and even by private individuals as well[14].it is also worth noting that under Cr.PC, no court order is required unless the entity is seen to be a "postal or telegraph authority" and generally e-mail providers and social networking sites are not seen as such[15].

Times today have raised a question on the laws applied and the system's success in regulating the curbing of Privacy Rights. Not only India but other countries worldwide are facing with the identical contentious issue as the existing laws are proving to be inapt.

[12] Hukum Chand Shyamlal Vs. Union of India and others, 1976 AIR 789, 1976 SCR (2)1060
[13] B.S Dala, Indian Centre For Communication Security Research and Monitoring (CCSRM), May 17, 2011 http://ictps.blogspot.in/2011/05/indian-centre-for-communication.html last viewed on 24/12/2013 at 10.29 PM
[14] Supra note no. 5
[15] Pranesh Prakash ,How Surveillance Works in India, July10,2013 http://india.blogs.nytimes.com/2013/07/10/how-surveillance-works-in-india/?_r=1

Right to Privacy in India:

The right to privacy includes the right to confidentiality of communication, confidentiality of private or family life, protection of honour and good name, protection from search, detention or exposure of lawful communication between individuals, privacy from surveillance, confidentiality of banking, DNA samples and other samples taken at police stations and other places and protection of data relating to individual.

The word privacy describes '*the rightful claim of the individual to determine the extent to which he wishes to share himself with others and his control over time, place and circumstances to communicate with others'*. Privacy is the condition or state of being free from public attention to intrusion into or interference with one's acts or decisions[16].

Right to privacy also is inserted as *'right to be let alone'*. The Right is not enumerated as a fundamental right in the constitution but has been culled by SC from Art. 21 and several other provisions of the constitution read with directive principle of state policy.

The movement of recognition of right to privacy in India started with ***Kharak Singh v. State of Uttar Pradesh and Others***[17] where, validity of chapter XX and some other provisions of the U.P police regulation were challenged as right guaranteed under Article 19(1)(d) and 21 of Indian constitution got violated . As a result SC declared, *'domiciliary visit*s' void and unconstitutional and concluded that Article 21 includes the right to 'protection of life and personal liberty'. This point was future enumerated ***Govind v. State of Madhya Pradesh and Another***[18]**,** by **Mathew J.** Later in ***R. Rajagopal v. State of Tamil Nadu***[19], the Supreme Court asserted that in recent time's the Right has acquired constitutional status. In, ***Malak Singh v. State of P&H***[20]**,** SC held the regulations that authorized surveillance for the prevention of crime and surveillance register as confidential documents. Despite of the lack of constitutional recognition, the right to privacy has long held a place in international charters on human rights such as Article 12 of Universal Declaration of Human Right, 1948. And Article 17 of International Covenant on Civil and Political Rights,1966 , which India has ratified[21].

[16] According to Black's law dictionary, 8th edition, Garner A. Bryan
[17] AIR 1963 SC 1295
[18] (1975)2 SCC 148
[19] 1995 AIR 264
[20] (1981) 1 SCC 420; 1981 SCC (Cri) 169
[21] Supra note 8

Cases evident of imbalance :

There have been various situations which are evident that India does not have a persuasive jurisprudence of privacy protection. The media has now made it possible to bring the private life of an individual into the public domain, exposing him to the risk of an invasion of his space of privacy.

In an authority case of **PUCL**[22]**,** in 1997**,** where issue of legal surveillance by the Central Authority arose and the constitutionality was Sec 5(2) of Indian Telegraph Act[23] was questioned. The court specified in judgment delivered, that "a telephonic conversation in private without interference would come under the purview of right to privacy as mandated in the Constitution. The court also observed that unlawful means of phone tapping are invasions in privacy and are uncivilized and undemocratic in nature". SC also gave the guidelines regarding the phone tapping[24] and pronounced of destruction and use of tapping records within 2 months.

Another famous incident of surveillance took during Ramakrishna **Hegde** regime in Karnataka in year 1988 where opposition alleged Hegde of ordering tapping of phones of opposition leaders and invading privacy. As a result, there was a huge uproar and was forced to step down as CM.Leaked Spy Files 3 reveals[25], after Mumbai Terrorist Attack 2008, Telecom Enforcement, Resource and Monitoring cells and Centre for Development of Telematics started preparing Central Monitoring System and the project would be manned by the Intelligence Bureau and agencies like RAW and CBI could access to it. Aim of it is to centrally monitor all

[22] AIR 1997 SC 568

[23] The Section 5(2) of the Act reads:
On the occurrence of any public emergency, or in the interest of public safety, the Central Government or a State Government or any Officer specially authorised in this behalf by the Central Govt. 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 and offence, for reasons to be recorded in writing, by order, direct that any message clear of messages to or from any person or class of persons, 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 detailed, or shall be disclosed to the Government making the order or an officer thereof mentioned in the order."

[24] The Supreme Court, in the same judgment, also went on to lay down various guidelines regarding phone tapping which are as follows:

i) If a telephone needs to be tapped, then the home secretary of the Union government or the respective state government can issue an order to this effect.
ii) Strong reasons have to be specified in order to issue such a directive.
iii) Such an order shall be in force only for two months unless there is another order, which will give the home secretary the right to extend it by another six months only.

Available at http://news.rediff.com/report/2010/apr/26/phone-tapping-what-1997-supreme-court-verdict-says.htm on 22nd Feburary 2014 at 3.50PM

[25] What Does Spy Files 3 Reveal About Surveillance In India? – CIS India, Center for Internet and society, 7th Nov, 2013 avilable at http://www.medianama.com/2013/11/223-what-does-spy-files-3-reveal-about-surveillance-in-india-cis-india/ last visited on 2nd mar 2014

telecommunications & Internet communications in India and would enable CDRs analysis and data mining to identify personal information of the target. This has not only questioned its legality but also the potential for abuse of Privacy Rights and other Human Rights. 'ClearTrail Technologies' brochure -the only leaked document on Indian surveillance technology by the Spy Files states that the company doesn't mention any compliance with Indian regulations in its brochure. Laws allowing for interception of communications could be viewed as controversial and in one way or the other the Government and intelligence department is curbing the privacy rights.[26]

The Hindu, in one of its article reveals that the Internet activities of India's 160 million users approx is already subjected to wide-range of surveillance, much of which is in violation of the government's own rules for ensuring 'privacy of communications'[27].

Most recent confrontation of the imbalance and irregularity of laws governing surveillance and privacy is one which happened in Gujarat. On November 15, 2013; a pair of investigative portals released a set of audio transcripts depicting an extraordinarily, all-encompassing surveillance of a young woman by Gujarat Police. This was done on orders of a political figure as her 'saheb' was obsessed knowing about her. Details were made public by websites *Cobrapost* and *Gulail* on the basis of tapped phone conversations revealed initiation of operation in August 2009. It also revealed, a Superintendent of Police, illegally listened to woman's telecommunications and deployed policemen at airport, hotel, and everywhere she went. SP, Singhal, revealed to CBI that surveillance was illegally carried out on oral instructions of Shah, BJP General -Secretary[28]. Incongruity being, the Gujarat police has twice refused to register a case against Chief Minister Narendra Modi and his assistant Amit Shah.[29] This

[26] Supra note no. 29

[27] Shalini Singh, Govt. violates privacy safeguards to secretly monitor Internet traffic, The Hindu, 9th September 2013 avilable at http://www.thehindu.com/news/national/govt-violates-privacy-safeguards-to-secretly-monitor-internet-traffic/article5107682.ece last visited on 27th feburary, 2014 at 10.36 PM

[28] Amit Shah deployed illegal Gujarat Police surveillance on woman for 'saheb': Cop, 15th November 2013, Times Of India, on http://articles.timesofindia.indiatimes.com/2013-11-15/india/44112353_1_gujarat-ias-young-woman-gujarat-police last visited on 9th February,2014 at 11.29 PM

[29] Snoopgate: Gujarat Police refuse to register case against Modi, Shah, 14th Jan, 2014, Times of India, on http://articles.timesofindia.indiatimes.com/2014-01-07/india/45954633_1_k-sharma-modi-and-shah-illegal-surveillance last visited on 9th Feb 2014 at 11.53 PM

snoopgate is cognizable and denial of the Gujarat police to register the FIR is against the Supreme Court's guidelines relating FIR.[30]

This is apparent that not only the State Government but also the Union government is equally at fault for dipping into its tyrannical reserves to allow a substantial erosion of our privacy.

This incident gives a clear picture that Privacy Rights is on a slippery slope as both BJP and Narendra Modi has been allowed to get away without giving any explanation for the tragic incident.

Today, violations of privacy, has become increasingly common, and aren't seen as repugnance to one's foundational civil liberties as *if you've got nothing to hide, you've got nothing to fear,* goes the argument for the act. But such a response thought acceptable as it may have come to become yet is inherently backward opposing all tenets of liberal, democratic polity.

Penalty for surveillance:

Lacking in law is not the end but also the penalties to be imposed on the Right violators are inadequate. Australia considers illegal surveillance, indictable offence punishable by imprisonment not exceeding period of 2 years and for unlawfully accessing stored communication: punishable by imprisonment of 2 years or penalty of 120 bugs or both[31].In India, where frequent curbing of privacy is there, penalty stands only 1 Lakh units. In a comment of proposal of Right to Privacy Bill drafted by government, Department of telecommunication said:

> "Section 51, financial penalty for unauthorized interception of communication may be increased from Rs 1 lakh to Rs 2 crore."[32]

[30] On 12th November, 2013 SC made it mandatory for police to register FIR for cognizable offence. A five-judge Constitution Bench headed by Chief Justice P Sathasivam said, "We hold registration of FIR is mandatory and no preliminary enquiry is permissible in cognisable offences." The bench also said that the "Police officials cannot avoid to register the FIR and action must be taken against them if no FIR is registered." http://archive.indianexpress.com/news/police-cannot-avoid-an-fir-in-cognisable-offences-supreme-court/1193935/ on 10th February 2014, at 12.24 AM

[31] Section 108(1) of Telecommunication Interception and Access Act available at, James Robert Watt, Electronic workplace surveillance and employee privacy- a comparative analysis of privacy protection in Australia and United States, p. 13.

[32] Avilable at http://businesstoday.intoday.in/story/dot-proposes-hiking-illegal-phone-tapping-penalty-to-2-cr/1/195443.html , last visited o 11.37 Am on 21st March 21, 2014

Reforms that could be introduced:

In *Right to Privacy Bill 2011*, presented before parliament, a sincere attempt has been made to define privacy and circumstance under which the government can conduct surveillance furthermore penalties for the misuse of data collected is also clearly defined.[33]Moreover, u/s 3 of *Information Technology (Intermediaries guidelines) Rules*, 2011, it is proposed to observe mandatory due diligence by intermediaries to publish the rules and regulations, privacy policy, and inform the users of computer resource not to host, display, upload, modify, publish, transmit, update or share any information that — belongs to another person and to which the user does not have any right to or grossly invasive into another's privacy.[34]

The central government passed *Information Technology (Procedure and Safeguard for interception, monitoring and decryption of information) Rules, 2009* where it is laid that no person shall intercept monitor or decrypt any information available on any computer resources except an order from Home Secretary or Joint Secretary, Ministry of Home Affairs has been obtained to do so. According to Rule 4, central government has power to delegate authority to intercept, monitor or decrypt any information on any computer resource to any agency[35].In *Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011* the law makers have also attempted to define the sensitive and personal data and body corporate to provide policy for privacy and disclosure and information.[36]

Conclusion

Right to Privacy is at a stake, measures to safeguard it must be taken within time as Constitution of India is impaired. Moreover, awareness must be introduced among people that they do not deliberately curb the rights of the others. Further, the drafted rules and regulations must be implemented as soon as possible else illegal use of others personal data for the personal benefit of the private individuals would be carried on at a grand scale than its today.

[33] Right to Privacy Bill, 2011 available on http://bourgeoisinspirations.files.wordpress.com/2010/03/draft_right-to-privacy.pdf
[34] Rule available at http://www.cyberlawdb.com/docs/india/legislation/rules/section79_rules.pdf
[35] Rule available on http://www.cyberlawdb.com/docs/india/legislation/rules/69rules.pdf
[36] Rule available at http://www.cyberlawdb.com/docs/india/legislation/rules/section43A_rules.pdf