Electronic Surveillance System

Kapil Goel, Lalit Rawat, Nikhil Kumar
B.Tech Student, B.Tech Student, B.Tech Student
Computer Science and Engineering
Dronacharya College of Engineering, Greater Noida, India

***Abstract* - The growth of information technology as a means of electronic surveillance has led to a great deal of research which managers need to evaluate and apply to the workplace. To support this process, managers should understand the aspects that guide research motives. The assumptions of the investigators influence what questions are asked about electronic surveillance, how inquiry is handled, and how results are interpreted. Encapsulates research that employs different organizational perspectives in studying electronic surveillance, and attempts to support managers in applying this research on the job.**

***Index Terms* - Electronics, Information Technology, Stockpile control, Organisational theory, Surveillance**

I. INTRODUCTION

Surveillance means close consideration of a person or group especially the one who are under suspicion or the act or observing or the condition of being observed. Being a developing country, India has brought several changes into its policies on Information Technology and still a lot more changes should be done. With the spreading IT stratum, surveillance technologies has also been introduced such as internet surveyance, CCTV surveyance, telephone and e-mail id surveyance etc. despite, it is purely a start & in future, imaginably in 2 to 3 years, advanced technologies will be popularized, which foliole us to question if current Indian legal framework has plans as to surveillance and if the privacy of individual in India is insured. This article discourse about distinct provisions under distinct statutes which allow govt to control surveyance, various departmental figures doing surveillance and right to privacy of individual in India.

II. INCIDENT

1. Till date, many new govt agencies has been formed such as Central Controlling System, Govtal Intelligence Network etc. and they have formerly started surveiyance in information-space, telephone, e-mail, personal bulletins etc. In the October 2012, ‘The Hindu’ has liberated an interesting report stating that over 10,000 telephone phone calls and 1,000 email id’s are beneath the scanner.
2. B.Mr. Milind Deora, in August, 2011, Rajya Sabha informed that the govt has now acquired technology to monitor or block contents on internet and has also started surveillance on facebook and twitter walls.
3. C.In 2012, Blackberry finally agreed to allow govt agencies to access personal messages on Blackberry Messenger (BBM) after many proposals made by Indian Govt.Previously, BBM comes with an encryption key which allows users to access messages and only those who have the encryption key can have the access to read and send a messages
4. D. Also, many private companies are also monitoring the contents on their websites or commodities, for investigation e.g. Microsoft is observing all the messages which are communicated on its commodity Skype. This information is used for their consumer research but they are also in violation of privacy of every individual who uses Skype.

III. DEPARTMENTS RUNNING UNDER INDIAN GOVERNMENT FOR SURVEILLANCE

Recently, many departments and agencies have been settled, under govt of India, to do surveillance in cyber-space (where online communication takes place between computers or systems), on particular messages, e-mails, cell-phones or on social media. Being actively expanding country, India has to accomplish secure guidelines and regulations in order to protect IT industry as well as to protect privacy of every citizen.

But at this moment of time, the assurance of constitution itself viz. potential and operations of jurisdictions, situations under which surveiyance can be executed etc. and shield of reports to be conserved by them is unidentified Also the provendors beneath which they have established are a question. It is possible that the data kept by them is unidentified. Also the provisions under which they have established are a question. It is possible that the data kept privacy and safety at large.

National Intelligence Grid

National Intelligence Grid aims at linking information saved on servers and networks of different departments and ministries of govt so it can be accessible by any department and intelligence agency. National Intelligence Grid does not aim at storing any type of information in its own and will only provide a platform where communication between computers and networks of different departments can be taken place.

Crime and Criminal Tracking Network System (CCTNS)

Crime and Criminal Tracking Network System targets at clustering, saving, evaluating, dislocating, distributing of data among various police stations and with State Headquarters and police organizations. By using CCTNS, any police station will get complete available information on any criminal or any suspect stored on the servers of other police stations or departments.

Central Monitoring System

Central Monitoring System aims at monitoring every byte of transmission viz. txt messages, telephone calls, on-stream activities, social medias communication and constituents etc. CMS was rehearsed by the Telecom Prosecution, Resource Monitoring (TERM) and by the Center for Development of Telematics (CDoT) and managed by Intelligence Burea. Today govt is doing surveillance on Facebook and Twitter walls by using Central Monitoring System.

Unique Identification Authority of India (UID Scheme)

Unique Identification Authority of India (UID scheme) aims at providing a special unique identity to every citizen of India in which figure print and basic information of a person will be obtainable. UID scheme appears under AADHAAR Scheme of govt of India, & at present, UID of India has issued number of Unique Id's to the citizens of India and till now it has covered 28.11% of the total population and still going on.

Indian Computer Emergency Response Team (CERT-In)

CERT, functional since January 2004, is a nodal agency of govt in response of any computer security circumstance. CERT has been created under the provenders of IT Amendment Act, 2008 and since then working as govt agency. CERT is not exactly surveillance agency of govt but it is response team of govt in order deal with any cyber security incident all over India.

National Counter Terrorism Center (NCTC)

After 2008 26/11 attacks on Mumbai, there was a commitment of agency to war against terrorism as there was a failure on the part of intelligence departments in India. So the tender of NCTC was invented. NCTC will extract its capability from Unlawful-Activities-Prevention Act,1967 and it will be part of (IB) Intelligence Bureau headed by the director.

As seen above, different govtal departments are working or will soon be in effect for different purposes but the question that frequently asked is that how far the data collected by them is secured and what mechanism does govt provide to stop misuse of this information by any third party or any internal govtal body for constitutional determination. Do citizens of India have right to isolation and freedom of speech and communication as enshrined in Composition of India? India even though being many laws and orders passed for surveillance and protection of privacy but it still needs more strong policies on governance of IT sector and for protection of privacy of individual.

IV. Laws governing surveillance

IT sector in India is growing at very high rate and the biggest problem is that there are no specific laws that governing surveiyance in India. Although there are many accomplishments and rules transpired by legislature which governs surveiyance discursively, there is a requirement of particular laws as to operating of govtal bodies, their powers, protection of individual privacy and power of speech. Section 69 **IT Amendment Act, 2008** gives power to govt to hijack, monitor or decode any information stored on any computer resources for the reason of civic safety, civic order etc. but who shall be sanctioned to check this information is unidentified. Still, CERT-In has been made by excellence of IT Act, 2008 but CERT-In will be performed when there is any attack on Indian computers or resources or when any of Indian servers being wrecked or corrupted by any alien body or any individual within or outside India.

The **Indian-Telegraph Act, 1885** are also given powers to central or state govt to intercept any message if it is against public safety and since then, as various laws came into force, the govt has got power.

The govt bodies which are working have got indirect powers from many different rules passed by the constituiiton, Yet there is no such valid scheme passed by parliament in relation to surveillance and authorities who has power to monitor and block information for any computer expediency. The information stored by Central-Monitoring-System will only be accessed by govtal bodies like Intelligence Bureau, Research and Analysis Wing (RAW), Central Bureau of Investigation (CBI), National Investigation Agency (NIA), Central Bureau of Direct Taxes (CBDT), and Narcotics Control Bureau (NCB). But who has given this authority or when shall such surveillance will be done is the query. Indian legal framework has provenders related to electronic surveiyance but they are inefficient.

Also, **Right to Privacy bill, 2011** has been presented in the parliament and an attempt has been made by govt as to define privacy and under which circumstances the govt has power to conduct surveillance and what shall be penalties as to misuse of such information obtained by the way of surveillance.

Under this bill, the surveiyance can only be admitted by permission of Home Secretary, Ministry of Home Affairs, Govt of India.

On October 27, 2009, the central govt has passed **Information Technology (Procedure and Safeguard for checking, monitoring, and decoding of data) Rules, 2009** in which it was lsupport down 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 Rules, under Rule 4, it has been lsupport down that the central govt has power to delegate such authority to intercept, monitor or decrypt any information on any computer resource to any agency.

Also, **Information Technology (Procedures and Safeguards for blocking for access of Information by Public) Rules, 2009** has been passed by parliament in order to block access of any information on any computer resource by public. According to Rules, the govt has power to block any information if generated, transmitted, stored or received or hosted by any computer resource for any reasons mentioned in section 69A of the Information Technology Act, 2000 i.e. sovereignty and integrity of India, defense of India, friendly relation with foreign state, security of state etc.

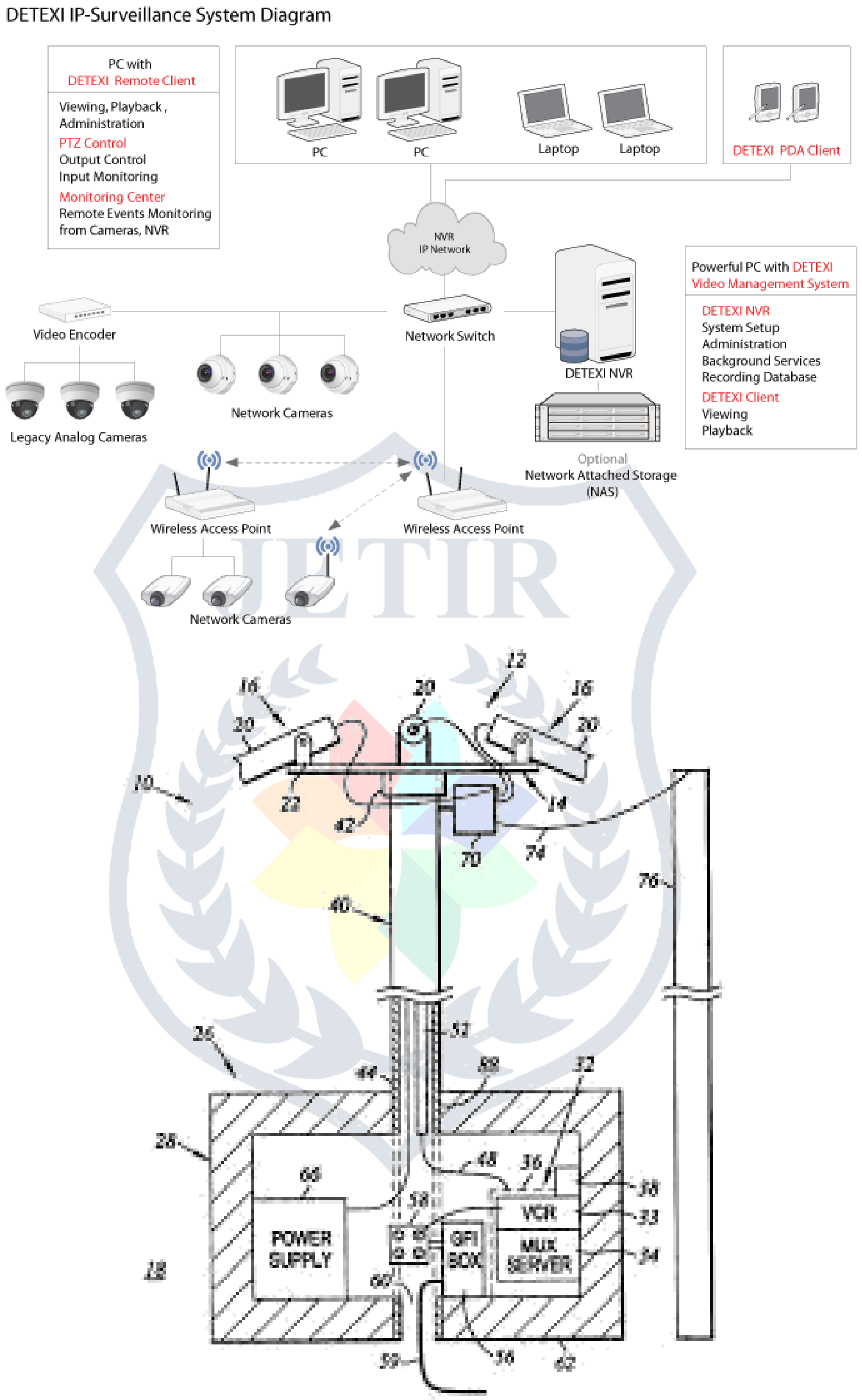
DETEXI IP-Surveillance System Diagram
PC with
DETEXI Remote Client
Viewing, Playback ,
Administration
PTZ Control
Output Control
Input Monitoring
Monitoring Center
Remote Events Monitoring
from Cameras, NVR
PC
PC
Laptop
Laptop
DETEXI PDA Client
NVR
IP Network
Powerful PC with DETEXI
Video Management System
DETEXI NVR
System Setup
Administration
Background Services
Recording Database
DETEXI Client
Viewing
Playback
Video Encoder
Network Switch
DETEXI NVR
Legacy Analog Cameras
Network Cameras
Optional
Network Attached Storage
(NAS)
Wireless Access Point
Wireless Access Point
Network Cameras
12
16
20
16
20
20
10
22
42
14
70
74
76
40
26
52
44
68
32
28
66
48
36
38
58
VCR
33
POWER
SUPPLY
GFI
BOX
MUX
SERVER
34
18
60
59
56
62

Fig 1

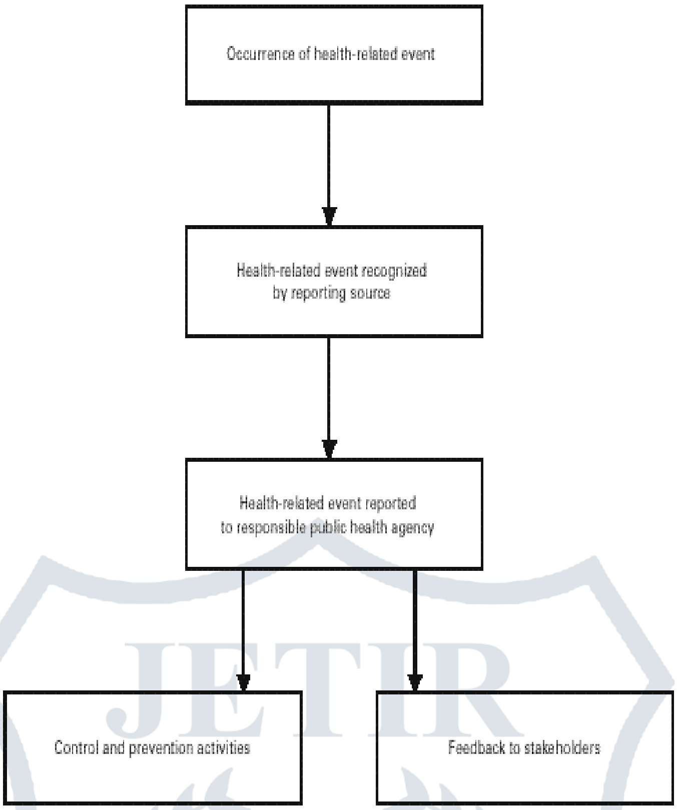
Occurrence of health-related event
Health-related event recognized by reporting source
Health-related event reported to responsible public health agency
Control and prevention activities
Feedback to stakeholders

Fig 2 Simplified example of steps in a surveillance system

V. USES AND PRIVACY CONCERNS OF TECHNOLOGIES

There are many different uses for GIS technologies, each can provide some insight into the different privacy and legal issues related to these technologies. GIS technologies are used to track cars and people; they are used for toll payment, in consumer products, and much more. RFID and GPS are gaining popularity, and deployed for convenience and efficiency in a wide range of applications. In addition to the growing uses of RFID and GPS, other seemingly unrelated technologies are being used for similar purposes. Each application of these technologies has its own set of unique privacy issues.

A. Vehicle Tracking

A **vehicle tracking system** combines the use of automatic vehicle location in individual vehicles with software that collects these fleet data for a comprehensive picture of vehicle locations. Modern vehicle tracking systems commonly use GPS or GLONASS technology for locating the vehicle, but other types of automatic vehicle location technology can also be used. Vehicle information can be viewed on electronic maps via the Internet or specialized software. Urban public transit authorities are an increasingly common user of vehicle tracking systems, particularly in large cities.

While police tracking of vehicles through added devices (e.g., beepers, GPS) has caused some controversy, vehicle surveillance can be done without attaching devices to the suspect's vehicle. Many cars already come with GPS devices that could be used for tracking, with the right authorization, or in emergency situations. For example, the General Motor's OnStar system gives operators the ability to use the GPS and cellphone components of OnStar to determine the precise location of the vehicle. With a warrant, this information could be used by law enforcement . Unfortunately, there is also vulnerability in such systems to the unauthorized use by hackers who could conceivably locate a vehicle without authority. Vehicle tracking is also made possible by ETC systems such as EZ-Pass and FasTrak. These systems usually utilize RFID technology, and they have GIS implications because they record where a vehicle is at a given time, as well as the direction in which the vehicle is driving and the timing of passing through toll booths. Traffic cameras at stoplights and on roads are vulnerable to such uses in similar ways, such as to match a vehicle with a location at a particular time. Many new cars come equipped with GPS navigation systems, ETC systems, and other technologies that can facilitate the tracking of vehicles. It seems clear that many drivers are unaware of these capabilities, and this should have a direct impact on any limitation the law imposes on their reasonable expectation of privacy while operating their vehicles.

B. Human Tracking

Finding a person who does not believe child safety is of the utmost importance is a very difficult thing, but the one thing many people disagree on is the method in which we monitor and protect our children from kidnappers, molesters and all of the other scum bags who prey on kids. For years, there have been rumors floating around about potential GPS micro chips that could be woven into a child's clothing or implanted slightly beneath the skin that would provide parents a way to monitor every location there child goes with relative ease. Although the truth about GPS microchip technology is nowhere near as sophisticated as it appears in Hollywood films, portable GPS tracking system are proving to be an effective and reliable solution to enhancing child safety, GPS tracking children can be one of the simplest and most efficient ways to boost the safety of any child, however, if you are a parent who honestly believes that a microchip can be implanted in your kid that will tell you everywhere he or she is at then you are very mistaken. It is true that GPS microchips are getting smaller and more advanced on almost a daily basis, but that does not mean the technology is anywhere near the level it is often depicted on science fiction motion pictures.

VI. Conclusion

Indian's growing legislative framework and surveillance policies are not adequate to deal with future threats and there is an urgent need to amend existing legal framework as well as to introduce strong and effective policies in order to protect IT industry as well as to protect privacy of individuals in the country. As referred above, UK and US have very effective policies and the workings of agencies as well as the laws relating to surveillance and privacy of its citizens. Similarly, in India, legislature should pass such acts and rules in relation to working of agencies, powers and authorities under whom surveillance will be done, protection and destruction of such data collected during surveillance and how far the privacy of individual is secured.

Also, the laws governing surveillance done by govtal departments and agencies which are currently working should be passed. There is also a need of defining the word privacy again in modern age as the development in IT sector and surveillance industry has changed the concept of privacy and laws governing it. The existing framework is not enough to deal with future threats and in future, there is a probability of increasing threats of cyber crimes and cyber terrorism. Although according to rules, the govt has got power to intercept, monitor, decrypt or block any information on any computer resource and also the central govt has got power to authorize any agency or any person to perform such activity as it thinks fit, but the working of such agency and who shall be employed in such agency has not been mentioned anywhere in the rules and also the provisions as to penalties for misuse of such information by any govtal body or person has not been given. It is possible that the information obtained can be used for political purposes.

VII. Acknowledgment

The electronic surveillance system is a result of a continuing process to which we have received valuable contributions from many colleagues at local and state level. The development of the indigenous software was funded through a grant support from Indian Council of whose support is duly acknowledged.

References

[1] Central Monitoring System (CMS): A data collection system similar to the NSA's PRISM program.It enables the Govt of India to listen to phone conversations, intercept e-mails and text messages, monitor posts on social networking service and track searches on Google.

[2] Lawful Intercept and Monitoring (LIM): A mass surveillance program used by the Indian govt to intercept records of voice, SMSs, GPRS data, details of a subscriber's application and recharge history and call detail record (CDR); and monitor Internet traffic, emails, web-browsing, Skype and any other Internet activity of Indian users.

[3] DRDO NETRA: Network that is capable of tracking online communications on a real time basis by harvesting data from various voice-over-IP services, including Skype and Google Talk. It is operated by the Research and Analysis Wing.

[4] NATGRID: An intelligence grid that links the databases of several departments and ministries of the Govt of India.

[5] Wright M. Automated surveillance and infection control: toward a better tomorrow. Am J Infect Control 2008.

[6] Stone PW, Dick A, Pogorzelska M, Horan TC, Furuya Y, Larson E.Staffing and structure of infection prevention and control programs.Am J Infect Control 2009.

[7] HotaB, Jones RC, SchwartzDN. Informatics and infectious diseases:whatis the connection and efficacy of information technology tools for therapyand health care epidemiology? Am J Infect Control 2008.

[8] Leal J, Laupland KB. Validity of electronic surveillance systems: asystematic review. J Hosp Infection2008.

[9] Atreja A, Gordon SM, Pollock DA, Olmsted RN, Brennan PJ, HICPAC.Opportunities and challenges in utilizing electronic hospital records for infection surveillance, prevention, and control. Am J Infect Control 2008.

[10] Furuno JP, Schweizer ML, McGregor JC, Perencevich EN. Economicsb of infection control surveillance. Am J Infect Control 2008.

[11] Meek J, Tinney SM. Computerize your infection surveillance for improved patient care—and savings. Health Financ Manage 2006.

[12] WrightMO, Perenvich EN, NovakC, Hebden JN, StandifordHC, Harris AD. Preliminary of an automated surveillance system for infection control. Infect Control Hosp Epidemiol 2004.

[13] Singer S, Meterko M, Baker L, Gaba D, Falwell A, Rosen A.Workforce perceptions of hospital safety culture: development and validation of the patient safety climate in healthcare organizations survey. Health Serv Res 2007.

[14] Dykes PC, Hurley A, Cashen M, Bakken S, Duffy ME. Development and psychometric evaluation of the Impact of Health Information Technology (I-HIT) scale. J Am Med Inform Assoc 2007.