International Journal of Law
ISSN: 2455-2194, RJIF 5.12
www.lawjournals.org
Volume 3; Issue 2; March 2017; Page No. 73-81

Surveillance and right to privacy: Issues and challenges

Ashok Kumar Kasaudhan

Assistant Professor, School of Law, Galgotias University, Gautam Buddh Nagar, Greater Noida, Uttar Pradesh, India

Abstract
This paper attempts to analyse the whether legislative framework relating to surveillance is adequate and able to balance between privacy of individual and defence and security of country. As an irony it is said that majority of Indians were safe from being victim of US Cyber surveillance programme PRISM not because they had kept themselves well-guarded against any possible breach of their privacy, but simply because they had not yet had a chance to be online. It also shows that even today most of the Indians have no access to computer and their non-access to resources and offline always ensured that they are protected from being victim of any covert operation of any surveillance agency. But surely this is not the matter to be consoled either by government or by citizens of India.

Keywords: surveillance, right to privacy, PRISM

Introduction

As an irony it is said that majority of Indians were safe from being victim of US Cyber surveillance programme PRISM not because they had kept themselves well-guarded against any possible breach of their privacy, but simply because they had not yet had a chance to be online. It also shows that even today most of the Indians have no access to computer and their non-access to resources and offline always ensured that they are protected from being victim of any covert operation of any surveillance agency. But surely this is not the matter to be consoled either by government or by citizens of India [1].

Surveillance means close observation of a person or groups especially the one who are under suspicion or the act or observing or the condition of being observed. Presently various types of technique is being used in order to check crime in cyber sphere. This is serious violation of one's fundamental right to speech and free profession. This also leads feeling of insecurity and chaos among citizen as when people are aware that their communication can be intercepted without any proper guidelines and laws they are not easy and free while communicating. The UN's Special Rapporteur on Freedom of Expression Frank La Rue delivered a report to the Human Rights Council outlining how state and corporate surveillance undermine freedom of expression and privacy. His report states that "*Privacy and freedom of expression are interlinked and mutually dependent; an infringement upon one can be both the cause and consequence of an infringement upon the other* [2]."

Although the India is world's largest democracy of the world and accordingly protects free speech and expression through its laws and constitution, still freedom of speech and expression is not absolute and privacy in online sphere is being restricted for many reasons. There are several reason for which speech and expression is being curtailed such as- defamation, maintenance of national security and communal harmony are major reasons for which they can be curtailed. They have very chilling effect over free flow of information in online regime, what has been provided by Constitution and other various statutes. Presently several mechanism including restrictive laws and technical means are being used to check the freedom of speech and expression that has undermined the position of India on world forum.

There are several challenge before free speech and expression in online domain in There are various sources from where challenges comes, the law which have most drastic effect is IT Act, 2000 and its Amendment and regulations in 2008 which was brought to combat with post-Mumbai attack. This introduced new regulations and measure keeping in view national security. In year 2011 certain new regulations were introduced which compels Internet Service providers to block the content within 36 hours of making complaint. It is immaterial by whom complaint is made. It may be made by an Individual, organisation or government body. This poses problems in many ways as in the case of liability of Internet Service providers (ISPs). It make him liable for which they should not be responsible at all as they are not author of the content and they have only provided platform. It is very tough task to have control over all contents and due to fear of being penalized of infraction of law they are extra cautious and this results in excessive censorship of the content. Nowadays it has been noticed that prosecution and arrest have been multiplied due to content which were considered as grossly harmful, harassing or blasphemous. Sometimes it has also been noticed that due to censorship, legitimate political comment were also considered as violating rules and regulations of IT Law.

Indian Computer Emergency Response Team (ICERT), a department of the Ministry of Communication and Information Technology that serves as a nodal agency for accepting and reviewing requests from a designated pool of government officials to block access to specific websites.2 This chapter will outline how takedown requests, both with and without court orders, are commonplace, and demonstrate that corporations sometimes contribute to censorship by over-complying with government requests. Along with filtering and blocking policies, these procedures are inconsistent and often threaten freedom of expression in India. With so many methods being used to restrict online speech, there is lively debate in India around how censorship affects fundamental freedoms and society. "There is no definition of what 'obscenity' and

'incitement' constitutes. Because of the vagueness of the law on the one hand, and the obligations of the law on the other hand [taking down offensive content], the door is opened to interpretation and subjectiveness," says Rajeev Chandrasekhar, a member of the upper house of the Indian Parliament. The vagueness of the law has led to people being arrested and charged for innocuous posts and tweets. The Information Technology Act (IT Act) and its 2008 amendments do not provide a clear legal definition of what is offensive and there is no common view in society of what can or cannot be said online and offline, leading to uncertainty. This has resulted in a growing tendency to report content deemed "offensive" and demand its removal. Intermediaries - web companies that host content but do not produce it – tend to over-comply with takedown notices out of fear of being liable for offensive content and then prosecuted. The over compliance of internet intermediaries with takedown notices is concerning as it removes from the internet content which is entirely legitimate. Compounding this problem is the lack of an appeal process. Intermediaries in India are neither required to notify people when their posts or photos are censored nor give them an opportunity to appeal the decision. In practice, this situation creates an indirect form of censorship when not the government but intermediaries become censors.

Right to Privacy [3]

Perhaps of all rights in the international legal catalogue, privacy is the most difficult issue to define. Depending on the context and environment, definitions of privacy vary widely. Protection of privacy is frequently seen as a way of drawing the line at how for society can intrude into person's affairs. The term 'privacy' has been described as the rightful claim of the individual to determine the extent to which he wishes to share of himself with others.

Privacy Technology and Surveillance [4]

Today much is written and spoken about the increasing level of surveillance which permeates about all aspect of our lives, with the consequential diminution of personal privacy. The Information commissioner who is responsible for United Kingdom's data protection and freedom of information legislation warned in 2004 against the dangers of sleepwalking into surveillance society. Introducing the report, a surveillance society, commissioned by his office and published in November 2006, the information commissioner went further:

Today I fear that we are in fact waking up to a surveillance society that is already around us. Surveillance activities can be well intentioned and bring benefits; they may be necessary or desirable. - For example to fight terrorism and serious crime to improve entitlement and access to public and private services, and to improve health care. But unseen, uncontrolled and excessive surveillance can foster a climate of suspicion and undermine trust. As ver more information is collected, shared and used, it intrudes into our private space and leads to decisions which directly influence people's lives. Mistakes can easily be made with serious consequences. False matches and other cases of mistaken identity, inaccurate facts and inferences, suspicions taken as reality and breaches of security.

Concern of these privacy implications of information technology was expressed by Lord Hoffmann when delivering his judgement in the House of Lords in the case of R v brown: My Lords, one of the less welcome consequences of the information technology revolution has been the ease with which it has become possible to invade the privacy of individual. No longer is it necessary to peep through keyholes or listen under the eaves. Instead more reliable information can be obtained in greater comfort and safety by using the concealed surveillance camera. The telephoto lens, the hidden microphone and the telephone bug. No longer it is necessary to open letters, pry into files or conduct elaborate inquiries to discover the intimate details of a person's business or financial affairs, his health, family, leisure interests or dealing with local or central government. Vast amount of information about everyone are stored on computers. Capable of instant transmission anywhere in the world and accessible on touch of a key board. The right to keep one too oneself, to tell other people that certain things are none of their business, is under technological threat.

The potential dangers were further considered by lord Brown Wilklinson VC in Marcel v. Metropolitan Police Commissioner. Documents belonging to plaintiff had been seized by the police in course of criminal investigation. Civil proceedings were also current in respect of the same incidents, and a subpoena was served on behalf of one of the parties to litigation seeking disclosure of some of these documents.. Holding that subpoena should be set aside, the judge expressed concern that:

If the information obtained by the police, the land revenue, the social security offices, the health services and other agencies were to be gathered in one file, the freedom of individual would be gravely at risk. The dossier of private information is badge of the totalitarian state.

Privacy and Surveillance

One of the main ways in which privacy can be threatened is by the act of placing an individual under surveillance. Surveillance can take a variety of forms. Physical surveillance is as old-established as society. At an official level it might involve placing individual suspected of criminal conduct under surveillance, whilst at the private level, reference can be made to the nosy neighbour looking at life through the corner of a set of lace curtains. In some instances, the success of surveillance may depend on its existence being unknown to its target. In some instances, the success of surveillance may depend on its existence being unknown to its target. In other cases, the fact that conduct may be watched is itself used as an instrument for social control. As George Orwell described in his novel 1984, the mere fact that people were aware that their activities might be subject to monitoring by the authorities would cause them to modify their behaviour, regardless of whether they were being watched or not.

Forms of Surveillance [5]

In 1971, Alan Westin in his seminal work, Information Technology in a Democracy, identified three forms of surveillance.

Physical Psychological, and Data

At that time it may be suggested, clear distinctions could be drawn between three categories.

Physical surveillance, as the name suggests, involves the act of watching or listening to the actions of individual. Such surveillance, even making use of technology, has tended to be an expensive undertaking capable of being applied only to a

limited number of individuals. In investigations subsequent to 7 July 2005

Authorities Working Under Indian Government for Surveillance

Recently, many departments and agencies have been established, under government of India, in order to do surveillance in cyberspace (where online communication takes place between computers or networks), on personal messages, emails, and cell phones or on social Medias. Being fastest developing country, India has to make strong policies and regulations in order to protect IT industry as well as to protect privacy of every citizen. The governmental bodies such as National Intelligence Grid, Central Monitoring System etc. have been setup for surveillance on internet, cell phones, private messages, as well as social media sites. But at this point of time, the protection of bodies itself i.e. powers and functions of authorities, situations under which surveillance can be done etc. And security of data to be kept by them is unknown. Also the provisions under which they have established are a question. It is possible that the data kept by these bodies can be misused by any private entity for any political or terrorist purpose which can endanger public 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 government 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 aims at collecting, storing, analyzing, transferring, sharing of data between 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 communication i.e. text messages, phone calls, online activities, social media conversations and contents etc. CMS was prepared by the Telecom Enforcement, Resource Monitoring (TERM) and by the Canter for Development of Telemetric (CDoT) and managed by Intelligence Bureau. Today government is doing surveillance on Facebook and Twitter walls by using Central Monitoring System.

Unique Identification Authority of India (UID Scheme) [6]

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 available. UID scheme comes under AADHAAR Scheme of government of India, and at present, Unique Identification Authority 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.

Recently population counting and their bio-metric updation has been has been central issue of debate as on the one hand this is related to welfare, security and surveillance mechanism of state on the other hand in absence of proper mechanism privacy and safety of individual is jeopardised. Currently intense debate is going on as to viability of UID. It has been introduced with a view to provide all the residents of India biometric based identification number. This is unique in the sense that it does not contain only figures rather it also contains some unique features of body such as iris, finger print etc. When figures are coupled with biometric identification they become more vital than ordinary information and are much prone to the breach of one's privacy. National Population Register (NPR) is a parallel body for the registration and maintaining data etc. But there is little bit difference between NPR and UID scheme as in the UID scheme data of residents is maintained while in the case of NPR data of citizens is maintained. In this way UID becomes an extricable component of surveillance regime in India.

Indian Computer Emergency Response Team (CERTIN)

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

National Counter Terrorism Center (NCTC)

After the attacks on Mumbai in 2008 aka 26/11 attacks on Mumbai, there was a need of agency to fight against terrorism as there was a failure on the part of intelligence agencies in India. So the proposal of NCTC was made. NCTC will derive its powers from Unlawful Activities Prevention Act, 1967 and it will be part of Intelligence.

Bureau Headed by the Director

As seen above, different governmental 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 government provide to stop misuse of this information by any third party or any internal governmental body for political purpose. Do people of India have right to privacy and freedom of speech and communication as enshrined in Constitution of India? India despite being many rules and regulations 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.

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 surveillance in India. Although there are many acts and rules passed by legislature which governs surveillance indirectly, there is a need of specific laws as to working of governmental bodies, their powers, protection of individual privacy and freedom of speech. 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 who shall be authorized to intercept this information is

unknown. Although, CERTIN has been made by the virtue of Information Technology Act, 2008 but CERTIN will only come into play when there is any attack on Indian computers or resources or when any of Indian servers being hacked or crashed by any foreign body or any individual within or outside India.

The Indian Telegraph Act, 1885 had also given power to central or state government to intercept any message if it is against public safety and since then, as various laws came into force, the government has got power. The governmental bodies which are working have got indirect powers from many different rules passed by the legislation. But there is no such legal framework passed by parliament in relation to surveillance and authorities who has power to monitor and block information for any computer recourse. The data collected by Central Monitoring System will only be accessed by governmental 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 a question. Indian legal framework has provisions relating to electronic surveillance but they are inefficient.

Also, Right to Privacy bill, 2011 has been presented in the parliament and an attempt has been made by government as to define privacy and under which circumstances the government 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 surveillance can only be granted by permission of Home Secretary, Ministry of Home Affairs, and Government of India.

On October 27, 2009, the central government has passed Information Technology (Procedure and Safeguard for interception, monitoring and decryption of information) Rules, 2009. In which it was laid 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 laid down that the central government 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 government has power to block any information whether 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, defence of India, friendly relation with foreign state, security of state etc.

Surveillance Laws in UK, US and Europe

United States of America United States has very strict policy on surveillance. In United States of America, the President has the power to grant electronic surveillance on any foreign power or any person who is agent of foreign powers. The President has the authority to grant such surveillance, without court orders, through Attorney General to acquire foreign intelligence information for a period up to 1 year. Attorney General shall report to the House of Permanent Select Committee on Intelligence and Senate Select Committee. Electronic Surveillance may also be granted by the court order. The Chief Justice will appoint seven judges from seven different circuit courts and this panel of seven judges will entertain such application of electronic surveillance and grant, modify or deny such application except in a case where such application has already been denied previously, the panel shall not entertain such application (USC § 1803). Any federal officer shall file such application for electronic surveillance

United Kingdom

In United Kingdom, Regulation of Investigatory Powers Act, 2000 governs the provisions for surveillance and investigation by governmental bodies. Regulation of Investigatory Powers Act gives guidelines to public authorities such as Police or governmental departments who want to obtain any private information. Under Regulation of Investigatory Powers Act guidelines, the surveillance and investigation can be done in case of terrorism, crime, public safety or emergency services. Surveillance includes full electronic surveillance such as intercepting communication on cell phones or emails or letters, GPS locations of target and access to electronic data encrypted or password protected.

Europe

In Europe, generally there are no direct laws provided to govern surveillance and EU members uses guidelines of UK's Regulation of Investigatory Powers Act as in Europe, right to privacy of individuals is highly developed area of Europe. Recently, in Europe, draft European General Data Protection Regulation 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. Also Data Protection Directive regulates the processing of personal data within European Union. But till now there is not specific laws governing surveillance laws in European Union except UK's Regulation of Investigatory Powers Act, 2000.

Information Technology Act Danger of Violation of Civil Rights [7]

"The Information Technology Act raises very real concerns. It demonstrates a legislature deeply sceptical of the internet, rooted in the conventions of the past, yet battling with the need for an information technology law in the present-day circumstances. This straddling of the known and the unknown has strange results. In its desperate need to bring in some security for activity on the net, it relies heavily on the executive, little realising that it can result in violation of civil rights particularly, in the light of India's infamous emergency. The absolute control it attempts to achieve over certifying authorities is worrying for the same reason. The act lacks balance."

Interception and Monitoring of Electronic Communications and Surveillance [8]

Security of the citizens is very important because state is the only saviour of the men and women who get affected only because of the negligence of the state.- Chanakya

During the attacks in Mumbai, the terrorists were reportedly 9in continuous contact with their handlers in Pakistan for several hours after the attack had begun. It was also noticed that terrorist used satellite and voice over internet Protocol

(VOIP) to remain in contact with their r handlers. In order to such untoward incident in future, IT Act, 2000 was amended in 2009 to avoid to tackle with such situations. The most important regime for Law enforcement agencies is that mechanism dealing with decryption, monitoring and interception be strong and robust so that it be feasible for enforcement agencies to collect data relating to terrorist activities. Before amendment in 2009 Section 69 provided government right to only to intercept data but after amendment in 2009 it has been extended to this power too inception, monitoring and decryption of data, monitoring and control of traffic data from computer resources as well blocking of websites which proved to be very controversial via virtue of Sections 69A and 69 B.

As for as telephonic conversation is concerned it is allowed under section 5(2) of Indian Telegraph Act, 1885 which provides that on the occurrence of public emergency or inthe interest of public safety the government has right to intercept any communications made through telephonic medium provided permission has been obtained from Union home secretary or principal secretary home.

The traditional method of intercepting data and blocking websites is at the router level and it is effectuated on the basis of IP address. However this is crude method an entire must be blocked just because of a small part of its content.

Deep Packet Inspection

A more sophisticated and complicated method is known as dep packet inspection. Deep packet inspection refers to interception of online data from emails, internet phone calls as well as data received from social networking sites such as Facebook, and Twitter etc. Every packet of online digitized data is intercepted, de-constructed, examined for keywords and then reconstructed within few milliseconds. This technology permits blocking of communications as well as the monitoring and modifying of information.

Deep packet inspection is a networking technology which is used to monitor and delay few types of content generated by computer applications such as peer to peer applications like Bit torrent and Lime wire.

In fact, the 2008 amendments to IT Act, 2000 were controversial in that the power to monitor and intercept information and block websites are traditionally associated with non-democratic societies and are inimical with Right to free speech provided by the constitution of India. However not only China, Iran but also democratic societies such as the US, Europe also engage in monitoring and interception of information.

One of the earlier developed systems for monitoring and interception of data is the Carnivore software platform in the US.

Carnivore Software [9]

US use the carnivore software as a monitoring mechanism over the internet which uses packet sniffing at the ISP level to monitor data through ISP level. Carnivore was Microsoft based workstation with packet sniffing software and a removable disk drive implemented in 1997 by the US Federal Bureau of Investigation (FBI). Carnivore is designed to monitor E-mail and electronic communications. It is known as customized packet data sniffer which can be used to monitor all of the internet traffic of a particular user.

Blocking of Websites

As it is known from several reports that leading IT companies of the world were forced to agree with demands of Chinese authorities in some point of time whether it be Google, Yahoo or Facebook. There is much data regarding the blocking of websites by the Indian Government, however blocking of websites by the Indian authorities has not been so widely reported Following lead of China India also begun blocking websites.

Misuse of Cyber Cafes

An additional issue which appears to be unique to India is misuse of cyber cafe for terrorist activities. In India unlike the western world computer penetration is still very low. For this reason most of the people visit cyber cafe to discharge their online activities. Initially Cyber cafe were considered to be tools of development for rural India as it brought drastic change to the growth of rural India by providing facilities like, e-learning, e-commerce and tele-medicine. However there is dark side too of the cyber cafes as it has been noticed by authorities that cyber cafes in India are being misused by terrorism related activities. In order to curb this menace in April, 2011 the Ministry of Communication and Information Technology, notified rules for the regulation of Cyber cafes all over India.

Right to Interception in Different Countries [10]

The *Government's* right to use surveillance, interception of electronic communications or traffic data retained by internet service providers is often questioned on the anvil of human rights principles. In most jurisdictions, this interference by Government is allowed in very rare and exceptional circumstances which are clearly specified either in the constitutional provisions or by a separate statute governing laws on privacy protection.The Magic Lantern Trojan horse project initiated post 9/11 attack in USA is reported to have been abandoned even though FBI used CIPA V a basic monitoring tool. In the United States, tinder the Communications Assistance for Law Enforcement Act, all phone calls and internet traffic are required to be available for uninterrupted real-time monitoring by Federal law enforcement agencies. In 2007, German federal police introduced `Bundestrojanee project but Federal Constitutional Court struck down the measure holding that trojanizing the computer of a suspect is constitutionally permissible only if actual evidence of concrete danger' exists and can be carried out under judicial authorization alone. The Open Net Initiative, collaboration between academic institutions that study filtering techniques, contains country reports and legal analysis of filtering trends on the internet. The Yale Center for Globalization or the Watchdog Group, Reporters without borders have questioned the technological company's activities that invade privacy and unauthorized collect data about individuals including from social networks. Another form of surveillance, known as Tempest uses reading electromagnetic emanations from computer devices in order to collect data from these systems from far off distances.

Recently ICC issued 'Global business recommendations and best practices for lawful intercept requirements' in 2010 which deals with guidelines on balanced approach for lawful interception. This policy statement comprising of eight specific recommendations, aim to balance the interests of Law

Enforcement Agencies, communication Service providers, business entities, consumers. The policy Statement recommends dialogue between governments and communication, erg ice Providers to define clearly lawful interception requirements, taking into account the 'obligations and benefits specific to communication service providers, maintenance of regulatory consistency, adoption of international technical standards availability of public funds for its infrastructure, and clear exposition of law and regulation.

Right to Interception in India

In India, section 69 of the IT Act, 2000 confers power on the central government or the state government to issue direction for interception, monitoring or decryption of any information through any computer resource to protect sovereignty or integrity of India, defence of India security of state, friendly relations with foreign states, or public order or preventing incitement to commission of any cognizable offence or for investigation of any offence. The subscriber or intermediary are obligated to render all assistance to the intercepting agency to secure access to a computer generating, transmitting, receiving or storing such information and to intercept, monitor or decrypt the information or provide information stored in computer resource. Section 69 A confers power on the Central Government to issue directions for blocking for public access of any information through a computer resource. Likewise, Section 69B empowers the Central Government to monitor and collect traffic data or information through any computer.

Right to Interception under Information Technology, 2000 Section 69

With respect right of interception, Section 69, the IT Act. 2000 confers power on the Central government or the State Government to issue directions for interception or monitoring or decryption of any information through any computer network. Section 69 provides grounds on which internet can be censored such as for national interest, in the interest of sovereignty or integrity of India, defense of India, security of state, friendly relations with foreign state, public order or the prevention commission of any cognizable offence or for any investigation purposes.

Section 69A

Section 69A prescribes provisions to block certain websites wherein the content is objectionable and is justified by the grounds mentioned in section 69. These provisions are justified as reasonable restrictions to fundamental rights guaranteed under constitution of India.

Section 69B

Under section 69B central government is employed to monitor, controlled traffic data or information generated, transmitted, received or stored in any computer resource. The provisions obligate intermediaries to render full cooperation in this for collection of data.

Rules Passed Under Information Technology, 2000 on Interception

Information Technology (Procedure and Safeguards for Interception, Monitoring; and Decryption of Information) Rules, 2009 were passed to lay down checks and balances and procedure to conduct interception. In order to ensure privacy is not invaded without due need for interception such interception requires prior approval from the competent authority *i.e.* Secretary in Ministry of Home Affairs, in case of Central Government and Secretary in charge of Home department in case of State Government (except. in emergency cases where separate procedure is provided). It prescribes maximum time of interception as 60 days and on renewal not to exceed 180 days. Rule 21 of the said rules places the obligation on intermediaries to ensure their employees maintain secrecy and confidentiality of intercepted communications and Rule 25 prohibits its disclosure except to the officer of authorized agency who" can use such information only for specified uses pursuant to direction of competent authority. Rule 23 prescribes destruction of intercepted communications after these are not required for law enforcement purposes. Similarly, the Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic Data or Information) Rules, 2009 were passed for governing activities of monitoring and collection of traffic data. Rule 3 of the said rules mandate prior permission of competent authority *i.e.* Secretary to the Government of India in Department of Information Technology under Ministry of Communications and Information Technology to conduct monitoring or collection of traffic data for cyber security reasons, inter alia, forecasting of imminent cyber incidents, tracking of persons and computer resource breaching cyber security. Competent authority can authorize any agency for the said purposes. In order to prevent unauthorized monitoring and maintenance of secrecy of information collected intermediaries are made liable for their employees by Rules 5, 6 and 11 of the said rules.

Freedom of Speech and Expression And National Sovereignty [11]

The Yahoo! France case

Yahoo is a reputed Internet Service Provider that. Renders various services from different websites. It operates a search engine, e-mail services, shopping, services or chat rooms on its online portals. Yahoo.com operates under the laws of United States. There are several regional Yahoo sites such as Yahoo France or Yahoo India with country code specific TLD (http://www.yahoo.fr; http://www.vahoo.co.in). The regional websites of Yahoo operate in the local language of the region and offer services to the local residents of the region and function under local laws.

Yahoo's auction site provides a service where any product can be put for sale and requests for bids from users. The Yahoo Services mails a notice to the highest bidder and seller to provide their contact details so that the sale transaction can be materialized and the seller and buyer can deliver the product on payment. Although Yahoo is not a party to the transaction, to a limited extent, it regulates the transaction by prohibiting specific items from sale through its website, for example, stolen goods, and illegal drugs, weapons. It also provides a rating system to monitor transactional experience of buyers and sellers on their websites. The users of Yahoo website are required to comply with the policies of Yahoo and to restrain from posting such items for buyers in particular jurisdiction where selling such an item would infringe the governing laws of the region. Yahoo does not monitor the content of every posting and in one of the cases, popularly known as the Yahoo France case, objectionable Nazi propaganda was posted on the Yahoo Auction Site.

The complaint in Yahoo! France case

La Ligue Contre Le Racisme Et l' Anti-Semitism (The League Against. Racism And Anti-Semitism and LICRA) served a cease and desist notice to Yahoo alleging sale of Nazi related items through Yahoo France Auction Site as violative of French Law. A complaint was filed by LICRA against Yahoo in the French Court. The French Court found that Nazi objects including Adolf. Hitler's book 'Mein Kempf was being sold on yahoo's auction site. French citizens could access these items on Yahoo.com or via a linking Yahoo.fr; The French Court held that Yahoo.com site is violative of Section R645-1 of the French Criminal Code that prohibits offering Nazi Propaganda and items for sale. The court passed an order on 12 May, 2000 directing Yahoo France and yahoo.Inc to remove access through Yahoo.com to the auction site offering Nazi Site items for sale.

Internet Censorship [12]

In India, reasonable restrictions on the right to privacy or in other words, censorship finds reflection many laws including Information Technology law, laws on phone tapping and interception. Section 69 of the IT Act, 2000 empowers a Central Government or a State Government to intercept, monitor, and decrypt information through a computer resource. Section 69A of the IT Act, 2000 empowers the Central Government to block from public access any information through a computer which it is satisfied that it is necessary to do so in the interest of sovereignty and integrity of India; defence of India, security of a state, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence. Section 69B empowers the Central Government to monitor and collect traffic data for maintaining cyber security. In India, IT (Intermediaries Guidelines) Rules, 2011 prescribes due diligence to be adopted AIM-discharging its duties. It obligates intermediaries to incorporate within its terms of use responsibility not to host, display, upload publish, transmit any information that belongs to another user unauthorised, information that is grossly harmful, harassing, offensive, defamatory, obscene, invasive of privacy, hateful, racial, encourages money laundering, or unlawful information. It also obligates users not to post or transmit any information that is harmful to minors, infringes any intellectual property rights, violative of law, use of spoofing or impersonation or containing virus that damage functionality of computer. It also puts obligation on users to check that such information does not threaten unity, integrity, and security of India, relations with foreign states, or public order or causes incitement to commission of any cognizable offence or prevents investigation of an offence or is insulting any other nation. The intermediary is under an obligation not to knowingly host or publish any such objectionable information and to remove it within 36 hours of complaint on actual notice.

Self-Regulation on Censorship

While on one hand the government's attempt to create a legislative framework to deal with internet censorship, on the other hand, some critics advocate usually the practice of 'self-regulation' both at the industry and at the user level. The Governments of certain countries such as UK, Canada, New Zealand encourage industry self-regulation. Although the laws of the offline world such as child pornography and racial hate speech also apply to the online world, Industry regulation includes creating technical devices that control access to content which is objectionable on the internet, particularly in regard to children using the internet. China has been reported to block access to Wiki leaks disclosing Beijing's fate over North Korea and allegations of hacking goggle. Similarly, in Saudi Arabia, Pakistan and Bangladesh Facebook was reported to have been blocked from access.

Internet Censorship in India [13]

In 2001 a Committee was appointed by the Bombay High Court to place recommendations on combating cyber pornography and crime. The Committee recommended licensing of cyber café, creation of ID Card system to ensure the authenticity of the users that avail its services. The Report also recommended that the Internet Service Providers maintain user logs. It also recommended that the minors should not be allowed to access adult websites and suggested that Internet Service Providers make available such software that protects minors. The training of cyber police personnel and establishment of special cyber-crime investigation cells was recommended. Many of these recommendations are being gradually implemented. Many states have established cyber-crime cells within the states and rules for proper functioning of cyber-cafe have also been recently passed, known as the IT (Guidelines for Cyber Cafe) Rules, 2011 that prohibit use of cybercak.' for pornography and other illegal purposes." However, many lacunas still exist in cyber law framework such as absence of prescribed data retention period for internet service providers and laws on employee surveillance and data mining. Further, in case cyber café breaches the prescribed laws and fails to render assistance in a law enforcement initiative in violation of Section 67C of the IT Act, 2000, the punishment is only up to 3 years and fine but constitutes a bailable offence. This does not prove a deterrent law and thus, cyber cafes continue to violate the laws. We need stricter laws to enforce the provisions effectively under IT Act, 2000.

Differing Socio-Legal Standards on Internet Censorship

Many jurisdictions adopt legal provisions of penal nature for censorship on internet. For instance, in some countries (including India and Australia), the website operators and owners who transmit any content unsuitable for minors are liable to pay penalty or undergo imprisonment. In certain countries such as China, active censorship policies block access to certain content which is unsuitable for adults too (contrary to the position in United States where adult content is not censored and only child pornography is censored). In this category fall other countries including Saudi Arabia, Singapore, United Arab Emirates and India. In China, the self-censorship initiative was recognized through the 'Public Pledge of Self-Regulation and Professional Ethics for China Internet Industry' issued by the Internet Society of China. The 'Public Pledge' encourages its members to comply with laws, promote safe and sound netiquette, and internet use practices.

NATGRID to Track NETIZENS

Recently, the Indian Home Ministry also declared its proposal to set up a National intelligence Grid (NATGRID) to track individuals who surf the Internet. The system would be implemented in three phases within two years and involve 11 central agencies including Central Bureau of Investigation, IB,

RAW, Enforcement Directorate, National Investigation Agency, Directorate of Revenue Intelligence and Narcotics Control Bureau which will have access to the data as and when required. Unless such a system gives due consideration to privacy concerns of citizens and

Pre-Filtering Internet Content [14]

Of late the issue of pre-censoring the third party information illegal content within 36 hours from actual notice or knowledge of the content if they do not monitor or edit content posted by third parties. Social networking sites contended that due to magnitude of content posted on daily basis such filters and pre-censoring was not possible on technical and administrative standpoint. If government proposes to pre censor such third party content, then as proposed hereinbefore clear rules that define ambit and scope of such regulation, including due diligence process for filtering by intermediaries ought to be passed and its technical and administrative feasibility also should be considered. The scope of ambit of terms "harmful to minors", "harassing" "hateful" found in Rule 3 of IT (Intermediaries Guidelines) Rules, 2011 may be clarified with help of illustrations as found in the Indian Penal Code, 1860. For example, on consumer blogs complaining about deficient services of a service provider is protected by free speech so long as it does not use abusive language or becomes defamatory. The meaning of terms used in Rule 3 can either be clarified by judicial decisions or explained by Parliament through illustrations as in case of Indian Penal Code, 1860 or through Government's clarifications. Further, netiquette needs to evolve in cyberspace so that users are aware and are able to distinguish form of free speech that is protected and content that becomes illegal. In a recent case a civil judge of a court in Delhi granted *ex parte* injunction against social networking sites that published defamatory content about gods and allegedly hurt the religious sentiments of Indian community. The court had the power to grant such injunction orders in order to maintain ' public order' as Article 19(2) of the Constitution of India allows reasonable restrictions on the right to freedom of speech and expression. Social networking sites are under an obligation to remove the objectionable content since the same has been brought to their actual notice and by virtue of Section 79 such content ought to be removed by an intermediary on receiving actual knowledge.

Phone Tapping Law in India

In India, in the famous *PUG*, case," petitioner challenged the State's power to tap phones under Section 5(2) of Telegraph Act. The court laid due emphasis on allowing phone tapping in serious situations that require protection of national sovereignty and interest, public order, incitement to commission of an offence friendly relations with states, or security of state. At the same time it observed that adequate mechanism to safeguard privacy should be in place through framing proper rules to avoid its misuse. The Section contains safeguards for interception through requirement of documentary formalities and placing various checks and balances through maintenance of records, appointment of a review committee and automatic expiry of interception order on expiry of 90 days from order date. These rules reflect rules for interception recently enacted under Section 69 and 69B of the IT Act, 2000. Since then many instances of phone tapping have been reported such as TATA controversy where newspapers published transcripts of Nasli Wadia's conversation about extortion money paid to ULFA leaders and tapping of phones of politicians was also reported. The question whether phone tapping constitutes invasion of privacy was considered by the Supreme Court in *R.M. Malkani* v *Suite of Maharashtra* [15] wherein the court held that telephone conversations of an innocent citizen shall be protected against unlawful tapping but the said protection is not available to a guilty citizen against law enforcement initiative directed at preventing corruption among public officials. In the aforesaid case the court took the view that there was no unlawful interception or irregularity in procedure adopted to obtain tape-recordings of conversation under challenge. The precedents in India on phone tapping indicate a trend that does not restrict government's power to intercept but in turn place procedural checks to check proper interception. This trend is evidenced from the recent case of *State of Maharashtra v Bharatilal Shah* [16] *wherein* the court dealt with a matter challenging the constitutional validity of the Maharashtra Control of Organized Crime Act, 1999 and provisions contained under Section 13 to 16 of the impugned act authorizing interception of communication and assessed if these were violative of the right to privacy. The court observed that interception of conversation amounts to invasion of privacy and such interceptions shall only he made in accordance with procedure established by law. The Court held that it is required that *"the procedure itself' must be fair, just and reasonable and non-arbitrary, fanciful or oppressive."*

Challenges to Right to Privacy in India

India is currently analyzing privacy and data protection challenges in introducing the Crime and Criminal Network and Tracking System (CCTNS) NAT Grid systems for better coordination between law enforcement agencies including police stations, to combat cyber-crimes. The CCTNS also aims to integrate e-filing by citizens in public authorities such as registration of births and deaths, application for licenses and has user login to access limited information available on the system depending on category of user who logs in. It is yet to be elucidated how much information will be available to different category of users on a CCTNS network. Introduction of Unique Identification System (UID) has also raised similar privacy concerns. According to UM, each person in India will be allotted one identification number by capturing his personal details by biometric means which will be unique to prove his identity. Critics of this model are of the view that UID number may be easily compromised at stages of collection, processing or storage and lead to proliferation of crimes: The centralized databases may technically fail or be unauthorized intercepted leading to a serious threat to privacy of individuals.

Repository of Electronic Signatures

Also, there needs to be a single repository of electronic signatures instead of multiple certifying authorities. As per the amended IT Act, 2000, Section 30 certifying authorities will substitute the controller as repository. Having multiple repositories will not be in interest of law enforcement as unless a unified repository exists. Checking frauds with respect to imposters and creation of fake electronic signatures will not be easily investigated. In the alternative there needs to be a mechanism where one repository can check other repository's records online for issuance of electronic signatures to a party so that one can verify that a person has submitted genuine

information to all repositories in case a person holds more than one electronic signature issued by the same or other certifying authority and has any history of frauds/cheating.

Conclusion

Hi this chapter,' we discussed the diverse legal approaches and regulatory framework adopted by different jurisdictions of fundamental rights of free speech and privacy on internet. The freedom of speech and expression on the internet in India is guaranteed by Article 19 of the Constitution of India and is regulated by reasonable restrictions permitted by the Constitution of India and the I T Act, 2000. The law on privacy of personal data guaranteed by Article 21 of the Constitution of India and data protection is an area which is still evolving in India and the legal framework is being strengthened to enhance data security and privacy in the online space through enacting appropriate rules under the IT Act, 2000. Despite being free, the internet in many ways is still territory specific when it pertains to freedom of speech and privacy law on the Internet. In this setting, legal framework, enforcement provisions, jurisdiction issue, and role of e-crime conventions become indispensable, particularly in cross border issues. Another emerging challenge in internet space is growing convergence in technologies, in form of VOIP, Internet messaging to mobile handsets, IPTV where telecommunications and broadcasting laws will need to be reanalyzed and aligned with laws for internet communications including law of interception, law against spamming, and other laws to protect privacy and data of netizens Recognizing this state, a new concept of net neutrality is gaining importance. Net Neutrality advocates that internet transmissions and law relating thereto should remain neutral irrespective of content and origin of communications flowing over internet. This debate addresses the pros and cons of net neutrality, related issues of surveillance powers and censorship of the internet and ISP liability and its impact. on further growth of Internet. A homogenized internet or convergence law will eventually lie required to govern the cyberspace. Yet at this point, it remains to be tested how much net neutrality can he *de facto* achieved! Having discussed the law on privacy and free speech protection, it is pertinent to discuss implications of breach of these rights, which leads us to the directly important subject of e-crimes.

References

1. Internet in the Age of Mass Surveillance: The Domestic Dimension. Aasim Khan and Nishant Kumar Published on Economic and Political Weekly. 2013; Vol XLVIII No.47.
2. India: Digital freedom under threat? Policy Paper, November 2013 Author: Melody Patry Editor(s): Mike Harris, Kirsty Hughes https://www.indexoncensorship.org /wp-content/uploads/2013/11/india_digital-freedom-under-threat.pdf
3. Edited by Verma S K and Mittal, Raman legal Dimensions of Cyber Space, Indian Law Institute, New Delhi page 198
4. Llyod Ian j. -<Information Technology law> oxford,, OUP, 5th edn, Page.
5. Ibid Page 76
6. Surveillance, Counter-Terrorism and Comparative Constitutionalism By Fergal Davis, Nicola McGarrity, George Williams available at https://books.google.co.in/ books?id=mz58agaaqbaj&pg=pa53&dq=authorities+working+under+indian+government+for+surveillance&hl=en&sa=x&redir_esc=y#v=onepage&q=authorities%20working%20under%20indian%20government%20for%20surveillance&f=false accessed on 02/04/2016
7. Information Technology Act: Danger of Violation of Civil Rights Author(s): Sruti ChagantiSource: Economic and Political Weekly. 2003; 38(34):3587-3595. Stable URL: http://www.jstor.org/stable/4413940 accessed on 3/4/2016.
8. Vishwanathan Aparna. Cyber law India and international perspective on key topic including data security, E commerce, cloud computing and cyber-crimes, LexisNexis, 2012 Page no. 147.
9. Christopher Rhoads, Loretta Chao Iran's Web spying Aided by western technology: Gear used in vast effort to monitor communications. Wall street journal, 2009.
10. Seth Karnika. Computer Internet and new technology laws, updated edn. 2013, LexisNexis page 285.
11. Seth Karnika. Computer Internet and new technology laws, updated edn. 2013, LexisNexis page 329.
12. Seth Karnika. Computer Internet and new technology laws, updated edn. 2013, LexisNexis page 82.
13. Ibid PAGE 335
14. India: Digital freedom under threat? Online censorship, https://www.indexoncensorship.org/2013/11/india-online-report-freedom-expression-digital-freedom-1/ accessed on 22/03/2016
15. AIR 1973 SC 157
16. 2009(1)ALT(Cri)173