Analyze The Legislative Framework relating to Surveillance and Right to Privacy: Issues and Challenges

Chhaya S Dule¹, Dr. Prof. Rajasekharai K.M ², B Prashanth³

¹Assistant Professor - CSE, DayanandaSagar University, Bangalore, Karnataka, India
²Principal and Professor - CSE, Kshatriya College of Engineering, Armoor, Nizamabad Dist., Telangana, India.
³Sumathi Reddy Institute of Technology for Women, Warangal, India.

¹chhaya.s-cse@dsu.edu.in

Abstract: 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 reasons 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. Under the Indian Constitution, the scope of Article 21 is multi-dimensional. The laws of torts, criminal laws as well as property law also contain a right to privacy in this paper to examine the adequacy and balance between the privacy of the person and the protection and the safety of the country within the legislative structure relevant to surveillance. It is ironic that the majority of Indians were protected from cyber surveillance PRISM not because they were well shielded from any potential violation of their privacy, but actually because they were not yet able to be online. It also shows that even today, most Indians do not have computer access and do not have access to resources to ensure they are covered of any covert activity by surveillance agencies. But this is definitely not something that the government or the Indian people would stabilize.

Keywords: Surveillance, Right to privacy, PRISM, legislative framework.

1. Introduction

It is more acute than ever before that it must solve the complexities of the digital age. The digital technologies, which are powered mainly by the private sector and which continually use people’s data, are increasingly penetrating the social, cultural, economic and political structure of modern societies. Increasingly potent technology such as big data and artificial intelligence threaten to establish an invasive digital world in which monitoring, analysis, prediction and even the handling of actions by both States and companies are performed in an unparalleled way. While the use of technologies based on data is not disputed, these inventions bring substantial risks for the integrity, self-reliability and privacy of humans in general if it is not handled with great attention. In particular, these technology developments are subject to great benefit. Most Indians today have no access to computers and are still shielded from covert operations of any supervisory agencies by their non-access and offline to resources but this is certainly not something to be comforted by the Government or by Indian people. Surveillance means close monitoring of an individual or groups, in particular of one that is suspected of being observed. Various forms of technology are currently used to monitor cybercrime. This
violates seriously one's constitutional right to freedom of expression and career. This also gives people a sense of uncertainty and confusion, because when people realize that communication can be intercepted without proper guidelines and rules, it is not simple and free when communicating.

1.1 Privacy and Surveillance:
The key technique to violate the security of privacy is through the tracking of a person. There are various forms of monitoring the activities. Physical tracking is as old as civilization, which means the illegal activity of an individual can be tracked under supervision on an official level. While the nosy neighbor could be referred to as seeing life in the coin of a number of lace curtains on a private level. In some cases, surveillance effectiveness depends on the fact that its purpose is not established.

![Figure 1.1 Surveillance Systems Strengthening Activities](image)

Above figure is surveillance information should be used locally to address and resolve problems related to control of communicable diseases and to strengthen evolving programmes. Monitoring and evaluation are keys to establishing and maintaining effective and efficient surveillance and response systems.

1.2 Scope of The Study:
The surveillance capacity of powerful computer systems has prompted calls for clear rules on personal data collection and management to create rights data security as a human right. If a person has the right to privacy, he or she has the right to data protection. Data security is a growing field as a result of technological development.

2. Literature Review

Lee, H.; Lee, Y.; Lee, K [1] The tool records every user's keyboard data and can be easily accessed from the Internet. New attack techniques, such as WinProc replacement, message hooking, philtre driver insert, object replacement disruption, IDT substitution of the descriptor interrupt table, direct polling and C / D exploitation techniques (control / data) bit vulnerability, were also implemented.

Lee, K.; Yim, K [2] In the PS/2 devices driver stack, a philtre driver will be inserted to steal keyboard data. The interrupt object replacement attack method replaces an object with a PS/2 keyboard interrupt and steals the keyboard information. The technique of an IDT replacement attempt to steal the data from the keyboard by replacing the PS/2 keyboard handling interrupt. There are three kernel techniques.

Lee, S.; Lee, K.; Yim [3] A defensive strategy is surmounted by an attacker executing a hardware-based attack. The technique for direct polling uses keyboard data by constantly accessing PS/2 keyboard input and output memory.
Ashok Kumar [4] Most Indians do not have computer access, their lack of access to resources and protection from the victims of any clandestine activity by the monitoring agency is always ensured offline. However, this is definitely not something that the government and people of India can encourage itself.

Ivana Stepanović, MA [5] this paper analyses how emerging technologies have changed the perception of the protection of private and public spaces, presenting many obstacles to maintain the right to privacy. These problems induced by the lack of a definition of personal privacy, and suggest that the term need to be reconsidered to establish a new working definition which makes it possible for basic human right, a major pillar of modern democratic society, is to be better secured against despotic forces.

F. Flammini et al [6] this paper presents a standard IOD architecture, which explains a range of problems related to protection and privacy required for safe and efficient sharing of data. It also discusses possible solutions that are suitable to the nature of IOD architecture.

Jayanta Ghosh [7] In these recent days, the constitutionality of data security and privacy has been so relevant. For this reason, a special status is required in the legal system. To offer a sophisticated defense to privacy concerns, the effectiveness of the existing legal system needs to be evaluated.

Babak Bashari Rada [8] this paper discusses the concept of big data and its ecosystem as well as the current problems in security and privacy, such as the systems, technology, application and data. The document also presents an outline for security and privacy issues in big data, allowing anyone in society to access the processing of massive data sets without renouncing their right to privacy.

3. Surveillance Strategy:
The monitoring approach depends on surveillance diseases, the goals and strategies of monitoring and how the surveillance information is used to inform public health policies and practices. A framework for early warning monitoring, such as a system that serves a monitoring function, should be implemented more comprehensively across sentinel sites. A small degree of integration and coordination may be required for efficiency in a multi-disease surveillance system. Some countries have also adopted a systematic approach to improving national monitoring systems through priority surveillance diseases, systemic evaluation of systems already existing, the development of system-building action plans, implementation of the surveillance and evaluation plans. In addition to determining whether the monitoring approach is ideally adapted to achieve the surveillance targets, the M&E must also evaluate success and obstacles in implementing the strategy.

Surveillance quality: The quality of the surveillance system is defined by attributes such as completeness, timeliness, usefulness, sensitivity, positive predictive value (PPV), specificity, representativeness, simplicity, flexibility, acceptability, and reliability. In the context of surveillance, the changes in the parameters will be established over time, and annual reviews will determine the degree of progress in the consistency and efficiency of tracking processes, data produced and the nature and standard of response to the information on public health. Monitoring characteristics can be measured in both quantitative and qualitative approaches. Some of the methods are outlined in the revised guidance for the assessment of systems of public health monitoring provided by the United States Centers for Disease Control and Preventions (CDC) and in the guide for the assessment of early outbreak detection systems. Annex 3b provides indicators pertaining to control device features.

3.1 Privacy and Surveillance
Most statements are written and spoken today about the increased degree of control that permeates all facets of our lives, with a consequent reduction in personal confidentiality. In 2004, in charge of United Kingdom data privacy and information freedom regulations, the Information Commissioner warned against the risks of joining a sleeping community in monitoring today that we are already waking up to a supervisory society around us. Monitoring practises can be well-intentioned and can be beneficial, necessary or desirable. For instance, the battle against terror and violent crime, enhancing rights and access to public and private services as well as enhancing health care. Unseen, unregulated,
intrusive monitoring can, however, cultivate and undermine an environment of suspicion. As more knowledge is gathered, exchanged and used, it penetrates our private space and contributes to decisions that impact people’s lives directly. Errors with severe implications can readily be made. False matches and other incorrect identities, misleading proof and conclusions, suspicions considered as facts, and violations of security. In his judgment in the House of Lords regarding R v brown, Lord Hoffmann expressed concern for these privacy implications of informational technologies. One of the less welcome effects of the IT revolution was the ease with which privacy of the person was overwhelmed. The individual user is no longer haveto look at or listen under the eaves. Instead, the use of the secret surveillance camera will achieve more assured information in greater comfort and protection. The pictures, the secret cell phone and the phone bug. It is no longer appropriate to open letters, pry files or carry out elaborate investigations to find out the intimate information about a person’s company, financial, health, family, leisure or centrally controlled affairs. A great deal of knowledge is stored on computers regarding everything. Able to transmit instantaneously anywhere in the world and open to a keyboard touch. The right to preserve one another, to say to others that certain things are not one of your businesses, is under technological threat.

3.2 Indian Government for Surveillance:
Recently, several departments and agency organisations have been set up, under the Indian government, in order to track cyber-space, personal and e-mail messages, mobile phones or social media, where online contact between computers or networks is carried out. India must follow the best policy and regulations to protect the IT sector as well as the privacy of all people as a rapidly developed country. The authorities like the National Intelligence Grid, the Central Monitoring System etc. have been established for monitoring on the internet, mobile telephones, private communications and social media sites. However, at this period the security of bodies themselves i.e. authorities’ powers and duties, the circumstances in which monitoring will take place, etc. And data protection is not considered to be held by them.

3.3 Challenges to Right to Privacy in India:
In order to enhance cooperation between law enforcement agencies, including police stations, to tackle cybercrime, India is currently studying the problems of privacy and data security with the establishments of the NAT Crime and Criminal Network and Monitoring System (CCTNS). The CCTNS 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.

3.4 Overarching framework protecting against undue Interference:
To handle personal information by both states and private parties, the regulation set up constituted as one pillar is required referred as State privacy private parties. Although state has power to determine the analytical mix of corporate personal information initiatives. Article 17(2) of the international Covenant on Civil and Political rights stipulates that individuals have to be protected by law. The increased interconnection between the public and private information processing and track record to date, which includes mass, repetitive abuse by certain companies, confirms that legal steps are required to achieve an acceptable degree of security of privacy. There is growing global agreement on minimum standards for the processing of personal data by governments, corporations and other private
players. The 1990 guidelines for the Regulation of Computerized Personal Data Files, the 1981 Council and Council of Europe Convention for the Protection of Persons with regard to Automated Personal Information Processing, and its modernized version, which provides a high degree of international protection, comprise International Instruments and Guidelines reflecting that development; These standards have informed the privacy frameworks of many states, especially the Convention for the Protection of Individuals, and can guide the design of adequate policy instruments.

4. Interception and Monitoring of Electronic Communications and Surveillance

Security of the citizens is very important because state is the only savior of the men and women who get affected only because of the negligence of the state. During the attacks in Mumbai, the terrorists were reportedly in 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 handlers. In order to such untoward incident in future, IT Act, 2000 was amended in 2009 to avoid tackling 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 is feasible for enforcement agencies to collect data relating to terrorist activities.

4.1 Carnivore Software:
The Carnivore software is used by United States as a monitoring mechanism over the internet which uses packet sniffing at the ISP level to monitor the data. 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.

4.2 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.

4.3 Problem 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.

4.4 Cyber Surveillance as an interference with the right to privacy of communications:
Computer and network control are used to track computer operations and data stored on a hard disk, or to move data through computer networks, such as the Internet. These regulations are carried out by states, businesses, criminals or individuals which are performed in hidden manner. This may be legal or may not require approval of a court or other independent government agencies. Article 17 of the ICCPR forbids 'arbitrary or unauthorized infringement of the privacy, home or correspondence' and obliges any State Party to develop legal mechanisms, including appropriate complaint structures and remedies for breaches of this rights. The HRC has made it clear that 'de jure and de facto confidentiality must be maintained' Correspondence 'shall not be intercepted and opened or read
otherwise to the addressee. The Committee's definition of the meaning of the word "correspondence" clearly encompasses the NSA / GCHQ's digital communicational cyber surveillance since that concept includes all electronic communications, such as e-mail, instant messages and telecommunications.

Figure 4.1 Electronic Communications Frequency

The collection or retaining of personal information on computers, data banks and other devices by public or private bodies must be regulated by relevant national laws and protections. Electronic monitoring, wire-tapping and recording of communications 64% and 33.7% are prohibited The HRC interpreted the sentence "interference" narrowly to include any direct or indirect action[9-11].

5. Conclusion
In this research concluded that 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 reanalysed 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 internet 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.

6. References
[1] Lee, H.; Lee, Y.; Lee, K.; Yim, K. Security Assessment on the Mouse Data using Mouse Loggers. In Proceedings of the International Conference on Broadband and Wireless Computing, Communication and Applications, Asan, Korea, 5–7 November 2016.
[2] Lee, K.; Yim, K. Keyboard Security: A Technological Review. In Proceedings of the 2011 Fifth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, Seoul, Korea, 30 June–2 July 2011.
[3] Lee, S.; Lee, K.; Yim, K. Security Assessment of Keyboard Data: Based on Kaspersky Product. In Proceedings of the International Conference on Broadband and Wireless Computing, Communication and Applications, Asan, Korea, 5–7 November 2016

[4] Ashok Kumar Kasaudhan Surveillance and right to privacy: Issues and challenges International Journal of Law ISSN: 2455-2194, RJIF 5.12 Volume 3; Issue 2; March 2017; Page No. 73-81

[5] Ivana Stepanović, MA Modern technology and challenges to protection of the right to privacy annals FLB – Belgrade Law Review, Year LXII, 2014, No. 3.

[6] F. Flammini et al., “Towards Automated Drone Surveillance in Railways: State-of-the-Art and Future Directions,” Int’l. Conf. Advanced Concepts for Intelligent Vision Systems, Springer, 2016, pp. 336–48

[7] Seena Naik K and Sudarshan E 2019 Smart healthcare monitoring system using raspberry Pi on IoT platform ARPN Journal of Engineering and Applied Sciences 14(4) 872-876.

[8] Mr. Jayanta Ghosh , Dr. Uday Shankar privacy and data protection laws in india: a rightbased analysis Bharati Law Review, Oct – Dec, 2016.

[9] Mahender K, Ramesh KS and Kumar TA 2017 An efficient ofdm system with reduced papr for combating multipath fading Journal of Advanced Research in Dynamical and Control Systems 9(Special issue 14) 1939-1948

[10] Babak Bashari Rada, Nafisseh Akbarzadeh Security and Privacy Challenges in Big Data Era International Journal of Control Theory and Applications ISSN: 0974-5572 Volume 9, Number 43, 2016

[11] Rajasri I, Gupta AVSSKS and Rao YVD 2012 Structural aspect of symmetry and its effect on generation of Planetary Gear Trains Applied Mechanics and Materials 110-116 2619-2622 10.4028/www.scientific.net/AMM.110-116.2619