Saudi Journal of Humanities and Social Sciences (SJHSS) **ISSN 2415-6256 (Print)**
Scholars Middle East Publishers **ISSN 2415-6248 (Online)**
Dubai, United Arab Emirates
Website: http://scholarsmepub.com/

Dilemmas of the Information Technology Era: Security Surveillance Vs Privacy Issues

Dr. Rehana Parveen*
Assistant Professor, College of Law, Prince Sultan University, KSA

***Corresponding author**
Dr. Rehana Parveen

Article History
Received: 14.03.2018
Accepted: 25.03.2018
Published: 30.03.2018

DOI:
10.21276/sjhss.2018.3.3.13

Abstract: In the era of technology security surveillance is rapidly increasing in most of the nations worldwide. Continuous security threats to public safety and national security demand use of such systems. The surveillance is often carried out by governments or governmental organisations, but may also be carried out by corporations, either on behalf of governments or at their own initiative. Depending on each nation's laws and judicial systems, the legality of and the permission required to engage in mass surveillance varies. It is often distinguished from targeted surveillance. No one can deny the fact that electronic surveillance systems offer advanced functionalities which threaten the privacy of those recorded in the video. In order to increase the public acceptance of surveillance systems, it is important that they obey the law of the state where they are installed and that their deployment strikes a balance between security and the need to protect privacy. There is an urgent need to balance the usage of electronic surveillance against its negative impact on privacy. In this research paper researcher is trying to discuss privacy issues and legal requirements associated with electronic surveillance.
Keywords: Surveillance, Privacy, Information Security, Legislation, Data Protection, Storage, and Encryption.

INTRODUCTION

Privacy protection is a realistic issue in the world we are living in today. Privacy is at the core of civil rights from which all other human rights and freedoms flow.

Since the twentieth century, and particularly since 9/11, rapid deployment of information and surveillance technologies in the name of national security has grave implications for individual privacy rights. In this paper the author emphasises the need for more accountability on the part of the watchers and more expansive notions of privacy and security to uphold the well-being of individuals, society and democracy.

The classic definition of the privacy concept is that it consists of the 'right to be let alone' in terms of isolation from the scrutiny of others, the average individual living in a town or city enjoys vastly more personal privacy than did our ancestors living in small villages where every action was known to and a source of comment for neighbours. The right to privacy receives a measure of recognition in the European convention on Human Rights which provides that, "Everyone has the right to respect for his private and family life, his home and correspondence to an extent greater than with other basic human rights", the right to privacy must be subject to considerable qualification and, as epitomized in the ongoing debate concerning the allegedly intrusive nature of media activities, the right to privacy has to be balanced against other rights. One of the key distinctions drawn in discussions of the right to privacy is between an individual's private and public personae. In countries such as United States right to privacy ceases when an individual moves outside private property. In such circumstances, the act of watching an individual's movement tends to be considered under the title of 'surveillance'.

In the past, 'surveillance' has been considered something which is primarily carried out by or on behalf of society as a whole (government). Although the act of placing an individual under surveillance may of itself modify individual's behaviour patterns, in general surveillance is a means to an end which may significantly affect other interests of the data subject. An obvious example might be the surveillance of an individual suspected of involvement in criminal/illegal activity. The act of surveillance may often lead to arrest, interrogation, trial and imprisonment.

THE MEANING OF "PRIVACY" "SECURITY"AND "SURVEILLANCE"

A. Privacy: Privacy is a right in many aspects. Although the uniform approach of privacy is often

seeked out. The opinion that there are not only one but many privacy rights is becoming more commonly accepted. Despite the fact most people have some familiarity with the concept of privacy, expert commentators report that defining privacy is a difficult, and perhaps impossible, task. This is due to the breadth of the concept of privacy. It covers several overlapping notions, including secrecy, confidentiality, solitude of the home, control over information about oneself, and freedom from surveillance.[1] Alan Westin provided one of the most cited definitions of privacy: 'Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others [2]. Altman defined privacy as an individual's ability and effort to control social contacts [3]. The right to privacy receives a measure of recognition in the European convention on Human Rights which provides that, "Everyone has the right to respect for his private and family life, his home and correspondence to an extent greater than with other basic human rights"[4].

The nature and moral significance of "privacy" are difficult questions that have attracted significant philosophical attention [5]. There is disagreement over whether "privacy" actually refers to something fundamental and coherent or simply groups together diverse issues that have a superficial connection [6]. Accepting that the concept of privacy is a coherent and useful one, various writers have proposed definitions of privacy. It has been variously described as a person's claim to determine what information about him or herself is communicated to others, a person's measure of control over personal information and over who has sensory access to him or her, and a state or condition of limited access to the person [7]. Although these descriptions assist in identifying the nature of privacy, it is still necessary to explain why it should or should not be protected. Here again, there are various explanations of why privacy is important. Privacy is said either to promote or to be a necessary component of human interests of inherent value such as human dignity, autonomy, individuality, liberty, and social intimacy [8]. A person who is completely subject to public scrutiny will lose dignity, autonomy, individuality, and liberty as a result of the sometimes strong pressure to conform to public expectations [9]. In addition to freedom from the pressure to conform, privacy also protects the individual from another party's use of his or her information to manipulate, out-compete, or otherwise exploit the individual. The value of privacy takes on another dimension as a result of modern information technologies. A certain measure of privacy with respect to personal information used to be ensured by the technological limits on its storage, communication, and cross-referencing with other information. However, as information technology has become more sophisticated and efficient, it has become possible to collect and integrate large quantities of personal information. [10]. The systematic collection, from multiple sources, of large quantities of personal information creates risks for individuals. While the risks mentioned in the preceding paragraphs flow from the disclosure of true and relevant information about an individual, dataveillance creates the additional risk that incorrect or unreliable data may come to be used to make judgments about whether to apply benefits or sanctions to individuals. In addition, as databases are integrated, data that was sufficiently reliable and relevant in one context may come to be used for inappropriately sensitive purposes. Westin suggests that there are two main sources of social pressure against individual privacy. The first is human curiosity or the seemingly universal "tendency on the part of individuals to invade the privacy of others [11]." Second, and more applicable in this context, is the use of surveillance "to enforce the rules of the society]." Since terrorism (particularly suicide terrorism) is not easily deterred by punishment after the fact, the pressure to detect and pre-empt terrorist plots is strong. Increased surveillance is therefore a predictable response to a dramatic terrorist attack.

B. Security: Security has been defined as an "absence of threats to acquired values" or a "low probability of damage to acquired values [12]." A distinction is often drawn between objective security and subjective security. Objective security refers to the low probability of damage, while subjective security refers to the feeling of security, or the absence of fear that acquired values are threatened [13]. The subjective component of security is highly relevant in the context of terrorism, which works primarily by inducing fear rather than by posing a real physical threat to most people. While one can have objective without subjective security (or the reverse), the two are related. It is possible that an incorrect subjective perception of risk may become an actual threat to objective security. This is because fear may produce counter-productive risk avoidance or destabilize society. On the other hand, an absence of justified fear may cause a person to run greater objective risks, with the same holding true at the national level. Security may thus require that one be objectively free from risk and also subjectively feel free from risk. The above-mentioned definition of security is very general. It does not specify the entity whose security is at issue (e.g., the individual, a group, the state, the international system, or the biosphere [14] or the types of values amenable to being secured. During the 1980s, the concept of security in political science was broadened beyond a concern with the security of the state (national security), which entailed a focus on international relations and military issues, toward the security of people as individuals or as collectivises [15]. The security of people ("human security") is understood to extend beyond national security, also including economic welfare, the health of the environment, cultural identity, and political rights. Thomas suggests

that human security incorporates both quantitative and qualitative aspects. The quantitative aspect refers to the satisfaction of the basic material needs essential for survival, including food, shelter, and health care, while the qualitative aspect refers to "the achievement of human dignity which incorporates personal autonomy, control over one's life, and unhindered participation in the life of the community[16]."

C. Surveillance: Due to the massive progress in technologies and systems, surveillance is becoming quite impossible to avoid. The notion of surveillance comes to us with a rich and textured layering of meaning. Its common definition is of close observation, especially the act of carefully watching a suspected spy or criminal or a place where an incident may occur. In other words surveillance is the act of watching the activities of people, with or without the consent of the people being watched, typically for management or security reasons. The technological development has ensured reduced hardware costs and increased levels of automation, so governments and law enforcement agencies worldwide consider surveillance a cost-effective method for fighting serious threats to public safety [17].

Observing or listening to persons, places, or ac tivitiesusually in a secretive or unobtrusive mannerwith the aid ofelectronic devices such as cameras, microphon es, tape recorders, or wire taps. The objective of electro nic surveillance whenused in law enforcement is to gath er evidence of a crime or to accumulate intelligence abo ut suspected criminal activity. Wigan and Clarke (2006:391) describe the term surveillance as "the systematic investigation or monitoring of the actions or communications of one or more persons." Surveillance is an act of continuous observation of a specific entity: over sustained period of time, o for a particular reason, with the aim of ensuring safety and security against unintentional or intentional dangers [18].

SECURITY VS PRIVACY ISSUES

Given that the security versus privacy trade-off appears to be biased in favour of national security, particularly in times of public insecurity, there is reason to fear that we may too easily sacrifice rights and freedoms such as privacy. Perhaps the bias in favour of security may be resisted by examining how privacy-reducing counterterrorism measures themselves reduce security. In this way, the trade-off analysis may be reframed as one between values that are more commensurable. Measures and programs intended to increase national security may actually reduce security in certain ways or for certain people.

Security Surveillance is very useful to government and law enforcement to maintain social control, recognize and monitor threats, and prevent/investigate criminal activity. With the advent of programmes such as Total information awareness programmes and advice, technologies such as high speed surveillance computer and Biometric software, and laws such as the Communications Assistance for law enforcement Act. It is an often made statement that we live increasingly in surveillance society, primarily manifest in the public's mind through the proliferation of CCTV cameras in our public and private spaces. Surveillance is both a crime prevention and detection measures, and has been greatly facilitated by developments in information and communication technologies. The nature of cyber crimes means surveillance is an important law enforcement tool in their detection and investigation. Surveillance may be carried out on a specified person's, or persons,' communication activities such as emails or file transfers; or of a 'virtual' location in cyberspace where communications are exchanged, such as chat room or bulletin board. The surveillance may be put in to operation at the edges of a network i.e. on a suspect's terminal equipment, such as computer or mobile phone; or within the network such as mail server, physically remote from the suspect [19].

From a legal perspective, a clear distinction needs to be made between surveillance activities carried out by public law enforcement agencies in the course of an investigation and those carried out by private entities, such as employer and land owner. As a state based activity, the former is governed by strict rules of criminal procedure to protect individual rights, specifically a person's right to privacy [20].

State authorized or Controlled surveillance may be carried out by personnel of the law enforcement agency itself, through the use of an informant, or require the involvement of a third party communication service provider to provide access to the forensic data, whether stared or in transmission and either created by the surveillance target or generated by the communication service itself The obtaining of data from a CSP is examined separately in the following section, since data obtained from, or with the direct involvement of a CSP, may not always comprise a form of surveillance subject to regulatory control. Obtaining data from CSPs has also required a distinct legal framework and raises unique issues of concern [21].

CONCLUSION & SUGGESTION

We are rapidly entering the age of no privacy, where everyone is open to surveillance at all times, where there are no secrets from the Government. The breaches of privacy by the Government in human sphere increase with geometric proportions. "Wiretapping" and "bugging" run rampant, without effective judicial or legislative control. Secret observation booths in government offices and closed television circuits in industry, extending even to rest rooms, common; offices, conference rooms, hotel

rooms and even bed rooms are "bugged for the convenience of government. Federal agents are often wired so that their conversations are either recorded on their persons or transmitted to tape recorders some blocks away....They have broken and entered homes to obtain evidence the dossiers on all citizens mount in number and increase in size. Now they are being put on computers so that by pressing one button all the miserable, the sick, the suspect, the unpopular the off-beat people of the nation can be instantly identified. The significance of the right to privacy has enormously increased in the present social set-up as a rapid development in the field of technology and communication which has vested us with numerous sophisticated electronic and computer devices that have increased the chances of direct and indirect intrusion in the area of an individual's privacy. Camera cell phones, mini cameras, mini microphones and other surveillance devices are just enemies of right to privacy as they are being used and would also be used in future to maintain a check over the right to privacy of citizens.

A society which values the individual's right of privacy will not tolerate unrestricted surveillance. Eavesdropping is an affront to personal dignity and inhibits individual action and expression. Because electronic surveillance is pervasive and indiscriminate, the unsuspecting victim is particularly vulnerable. Controls must be imposed which will keep pace with the rapid development of sophisticated electronic devices. Experience has demonstrated the difficulty of obtaining adequate legislation at the national and federal level. Nor is a satisfactory remedy found in the Constitution, for eavesdropping does not fall comfortably within the proscriptions of the Fourth and Fifth Amendments. The individual states are in a much better position to control surveillance.

Laws intended to govern domestic electronic surveillance now have an adverse impact on national security activities because they influence how cooperative the information service providers can be with the national security community. Laws such as the Electronic Communications Privacy Act and the stored Communications Act may create criminal and civil liabilities for the private sector that eliminate their motivation to assist in issues of national security. These laws provide needed protections for the privacy of ISP customers, but amendments must be made to allow the sharing of network security and threat information with the government.

But even when such controls are adopted at the state level, there is a remaining problem of enforcement. The needs of law enforcers and businessmen can be met if legitimate surveillance based on a standard of reasonableness is permitted. The exclusionary rule and firm judicial supervision will curb abuses. Heavy penalties for wrongful eavesdropping, or for possession of surveillance equipment with intent to eavesdrop, will prevent blackmail and other criminal activities. Adoption of the statutory controls suggested, and their enforcement by an informed judiciary will adequately preserve the privacy of individual communication. More and better public policy research on the use of the technology, its security and privacy implications, as well as the effects of regulation is needed.

REFERENCES

1. Overview of Privacy, Privacy International citing Simon Davies at 24 November 2008.
2. Gavison, R. (1980). Privacy and the Limits of Law. *The Yale Law Journal*, *89*(3), 421-471.
3. Altman, I. (1975). The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding.
4. http://www.echr.coe.int/Documents/Convention_ENG.pdf
5. Gavison, R. (1980). Privacy and the Limits of Law. *The Yale Law Journal*, *89*(3), 421-471.
6. Schoeman, F. D. (Ed.). (1984). *Philosophical dimensions of privacy: An anthology*. Cambridge University Press.
7. Swire, P. P. (2006). Privacy and information sharing in the war on terrorism. *Vill. L. Rev.*, *51*, 951.
8. Rachels, J. (1975). Why privacy is important. *Philosophy & Public Affairs*, 323-333.
9. Schoeman, F. (1984). Privacy: philosophical dimensions. *American Philosophical Quarterly*, *21*(3), 199-213.
10. Clarke, R. (1994). Dataveillance: delivering 1984. *Framing technology: Society, choice and change*, 117-30.
11. Westin, A. F., & Ruebhausen, O. M. (2015). *Privacy and freedom*. Ig Publishing.
12. Baldwin, D. A. (1997). The concept of security. *Review of international studies*, *23*(1), 5-26.
13. Hope, T., & Sparks, R. (2012). *Crime, risk and insecurity: law and order in everyday life and political discourse*. Routledge.
14. Rothschild, E. (1995). What is security?. *Daedalus*, 53-98.
15. Lipschutz, R. D. (1995). *On security*. Columbia University Press.
16. Thomas, C. (2000). *Global governance, development and human security: the challenge of poverty and inequality*. Pluto.
17. Rajpoot, Q. M., & Jensen, C. D. (2015). Video surveillance: Privacy issues and legal compliance. *Promoting Social Change and Democracy Through Information Technology*, 69.
18. http://www.encyclopedia.com/social-sciences-and-law/law/law/electronic-surveillance, Retrieved at 29.9.2017

19. Walden, I. (2007). *Computer crimes and digital investigations*(p. 01). Oxford: Oxford University Press.
20. Britz, M. T. (2009). *Computer Forensics and Cyber Crime: An Introduction, 2/E*. Pearson Education India.
21. Walden, I. (2007). *Computer crimes and digital investigations*(p. 01). Oxford: Oxford University Press.