© 2016 IJSRSET | Volume 2 | Issue 2 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Function Creep in Surveillance Techniques

Muhammad Safdar[1*], Faizan Ullah[1], Imran Khan[2], Farman Ullah[1], Izaz Ahmad Khan[1]
[1]Department of Computer Science, Bacha Khan University Charsadda, Khyber Pukhtoon Khwa, Pakistan
[2]Department of Computing and Technology, ABASYN University, Peshawar, Khyber Pakhtunkhwa, Pakistan

ABSTRACT

Surveillance practices have benefits. The surveillance gadgets are used for security purposes, making it easier for the security personnel to determine who, at what time and how an incident happened. However, surveillance practices have raised issues related to privacy. The government may use the surveillance gadgets to spy on the users. The information recorded by or on the various modes of surveillance can be compiled, disseminated at a high speed, and low cost. In the wrong hands, the information may be used in wrong ways that infringe on people's security and privacy. Function Creep has greatly harmed the privacy and has resulted in segregation and isolation among different social classes. Why and how it happens, what its implications on the society are and what possible solutions can be used to control it has been discussed in this paper.

Keywords: Surveillance, Data Mining, Privacy, Security, Data Surveillance, Function Creep.

I. INTRODUCTION

The development of technology has led to the improvement in the surveillance practices. The levels of security have improved such that using the surveillance gadgets, one can determine to whom, when, and how an incident captured by the surveillance gadget happened. This has created a sense of assurance to the public. However, this most celebrated method of assuring security has threats and risks. The issues associated with the surveillance practices have raised issues. This research explains what it is, why and how it happens, what its implications on the society are and what possible solutions can be used to control it. It has been found that function creep significantly undermines the rights of privacy; breeds control by its operators in the society and give rise to segregation and intentional isolation of different social groups of the society.

II. METHODS AND MATERIAL

1. Literature Review

Conflict related to surveillance practices has attracted the interest of many scholars and experts. Much information has been published relating to the ethical issues in surveillance technology. Many sources have acknowledged the fact that it infringes on the privacy of the people.

In [1], the authors look at the ethical implications of the use and proliferation of biometric identification systems. Like any other surveillance practices technology, the biometric identification is faced with ethical issues leading to conflict. The author feels that biometric identification should not be a mandatory practice that one needs to obtain documents such as driving license; however, it should be used to counter criminal activities. It should be voluntary practice. Whereas a person searching the biometric identification database will not be able to see the picture of the owner of the identity, there is no standard way to secure the information [1].

There is no limit to which the government can watch over the citizens. In [2], the authors feel that through surveillance practices, the government have found ways of intruding into the lives of its citizens. Technology allows people to compile, store, match, analyze and disseminate personal data at low cost and high speed. Whereas people are interfering with their privacy, the law is insufficient to protect them. There is conflict in the accountability, fairness and the infringement of people’s rights. In [9] the author argues that there are no regulations and data surveillance currently. The rules being enacted to counter the ethical issues of data surveillance are taking effect at much slow pace. Therefore, the author feels that the potential effects of both individual and mass dataveillance posture moral threats and need to be all the more nearly controlled by both people and the government [9].

On the subject of the legality scopes of surveillance technology, [4] examines the legal tools accessible to guarantee that privacy and individual information insurance are regarded in endeavors to guarantee the security of our general public. The creators figure out that changes are required in our legal and administrative system if privacy is to be sure to be regarded by law requirement powers and brainpower organs. Moreover, the creators contend that privacy sway appraisals ought to be utilized to deal with the need and proportionality of security and reconnaissance projects and policies versus privacy.

There is loss of privacy and consent in the digital era. In [6], the Privacy and consent in the digital agehave been examined. The article goes on to sets of five dilemmas that will need to be addressed in the search for solutions to the problem that has been brought up by the use of surveillance. As technological innovations gather pace, privacy and consent issues will continue to be at the forefront of the individual quest for cyberfreedom as well as institutional and business desire for control. [5] Discusses the loss of reserve, a critical component of privacy, caused by technological advances. The author defines define reserve as our ability to control what information about us is disclosed, and what is not. Therefore, [7] feels that the surveillance practices are not being used for the purposes they are intended for. The documents that were once used to show expertise or legality to do something are now being used for security purposes. This is a shift away from what the surveillance tool being used was meant for.

The aftermath of the dark days of 9/11 is an increase in surveillance. Security has been strengthened to an extending that it infringes on people’s privacy. [8] Reviews how post-9/11`security' issues converge with existing and emerging technologies, especially those identifying with personality, area, home, and work that will structure the foundation of the European Information Society. There are complexities produced by the way that these advances work destinations of patriot resistance and formal bureaucratic parts. A large number of the arranged reconnaissance strategies and innovations are union advances intending to unite new and existing information sources, yet are not able to do as such as a result of poor information quality and the trouble of utilizing the Incorporated information to diminish genuine wrongdoing risks [8].

Data mining has enabled the compilation of the information collected via surveillance method applied. Through technology such as World Wide Web, it is possible, via data mining to collect private information about a person. This poses more than a security measure but as a threat to people’s rights to privacy. [3] Examines the ethical issues involved in data mining. Although in business context data mining can be used to compile some personal data, which companies to build detailed customer profiles, and gain marketing intelligence, it poses threats and risks in the person's privacy and individuality. Data mining makes it difficult for a person to control unconventionally the dissemination and unveiling of data relating to his/her private life. [10] Examines the past, current and future uses of these technologies and examines the ethical issues that must be confronted when evaluating their impact.

Essentially technology of surveillance poses threats to people’s privacy. Although the information collected via the surveillance methods employed is used for the positive intention, the information in the wrong hands is a time bomb. The review of the literature shows that an effort has been made to identify and define some of the issues related to causing the concerns regarding our private and public life and image.

2. Common Surveillance Practices and Function Creep

Function creep includes expanding the utilization of an innovation from the foundation for which it was at first planned to an alternate reason [2, 3, 8]. This is promptly seen in the utilization of personality cards in the UK, presented in the 1939 National Registration Act for the reasons of security, national administration and apportioning. By 1950, the same cards were being utilized by 39 management organizations for reasons as different as gathering packages from the mail station routine police inquiries. While any or even these were apparently defended, few could be supported under the terms of the beginning Act. It was a mix of dissent and the inevitable recognition of this augmentation of utilization, which prompted the abrogation of the Act that same year. No doubt, the concept of surveillance technologies like CCTV is blessing for everyone from businesses to homes but at the same time it raised the issue of data protection and privacy. It is because of the fact that images and information of the innocent people can be broadcasted via internet or can be used elsewhere.

A. Facial Recognition System

As the name indicates it is computerized software used to identify the facial features automatically by matching them with the ones recorded in the database. This system is immensely important in recognition of facial features from video and the digital images. CCTV and FRS work in conjunction to ensure elite security to the masses. Studies have shown that CCTV alone failed to achieve the desired goal, so the engineers thought to incorporate FRS into CCTV to help ensure more security and surveillance especially in identifying crimes and other similar threats [11]. Though, it worked awesome as far as security is concerned but the use of FRS in CCTV gives birth to Function Creep.

However, when it comes to privacy, it is stated that the Face Recognition System violets privacy as the faces and other information like time, location and date are automatically identified by the system. The recorded information is passed on without the concern of that particular individual and the alarming thing is people are unaware of this concept. It is also said that the FRS special algorithms is more effective in identifying the minority groups i.e. darker people and the elderly as compared to the majority [6], thus leads to more privacy harm to this particular group than other individuals of the society.

B. Function Creep and Biometrics

Biometrics means human recognition. In technical words it is the process of measurement, recording and detection of personal attributes and physical characteristics of a person and then matching and sorting in the database to confirm or create the individual’s identify. Individual data is collected and recorded in the system and is used for verification and identification when needed. Biometrics system includes both personal and physical attributes for identification purposes. The physical description commonly involves DNA, fingerprints, thumb geometry, iris and retina structure [12]. However, advancement in technology has expanded it to bar codes and unique identification numbers. Similarly, the personal attributes includes typing process, voice characteristics and signatures etc. Naturally, every human being has four exclusive attributes e.g. DNA, finger prints, retina and iris structure. Being the unique attributes these are the common verification and identification tools in general. Biometrics systems has been used everywhere from defence to law enforcement, from restaurants to malls, from financial institutions to offices, from health sectors to social services and what not. This system is the epitome of security but it also violates the privacy. In biometric identification, an individual give private info about him/herself so, it raise several questions like who hold the data, what is the purpose of collecting the information and to what degree this information will be used. The immense use of biometric technology in everyday life make it subjected to Function creep. Actually Biometrics can give personal information other than the identification and that is the reason it is subjected to a number of questions. Information derived from the retinal scan of an individual can even give medical information of that particular person such as high blood pressure and diabetes and this info could be used in several unethical ways to achieve some economic gains [13].

C.

D. Function Creep and DNA

DNA- Deoxyribonucleic acid is a unique nucleic acid that holds the genetic code and is mainly used in forensic sciences to control violence. Through DNA testing a person can easily be recognized by matching saliva, blood, semen, skin and hair. This process of identification has been used since 1984 and since then used all across the world in forensic sciences to control crime. Advancement in technology has subjected DNA tests to function creep, as the DNA test of an individual not only identify the culprit but also give information about his/her kin. As DNA holds the genetic code and this code is the info rooted in human cells and has link with closed family members. Recognition of an individual via this link is termed as the familial searching. Such kind of links and information about family members lead to many serious issues [14]. Initially, there was no such thing involved in forensic sciences, so no rules are designed for it. Even after knowing about it many developed countries having large databases didn't made any changes in their terms and conditions.

No doubt, all these databases and the advancement in DNA tests are made with good intentions but still it raised many questions regarding privacy. Does the general public know about it? Did the forensic institute are willing to make any amendments in their terms and conditions? Every technology once implemented offers countless benefits for the well-being of the community, but its expansion and advancement leads to lesser legal control and results in function creep. Even if the loopholes and gaps are identified the course of regulating and changing the laws is quite slower, thus giving birth to function creep and at the same time violates the privacy of innocent people [18-24].

III. RESULTS AND DISCUSSION

Possible solutions and data analysis

We all know that these technologies are playing an important role in our lives but restricting the scope of these databases can guarantee privacy protection and give peace of mind to common man. The uses of every single database should be clearly defined to the concerned people and departments to avoid any kind of privacy violation [15].Implementing common law. Like if a particular database need to be shared with any other country or countries, the database should be used according to that common law made for this particular purpose [16, 17]. There must be ethical committees for every surveillance act. Moreover, the members of the committee should belong to different backgrounds and social groups.

A. Watch the Watchers

A technique known as servillance is said to be on contrary to surveillance. Under this general population has the authority to keep in check the officials that take charge of searching it. Main theme of introducing this procedure was to create a discussion over any contradictory method passed on by the authorities; however, the power its board holds is limited so to not encourage criminals from finding way out of their sentences via serveillance. The aim in going through this process is to assist in law making and preventing the use of illegally obtained evidence and proofs in courts, not to create further linked function creep. Presentation of data obtained via unlawful means has become a common practice now which needs to be taken care of. This is possible only by correcting the system and declaring laws that do not support function creeps in any manner. Living in a surveillance society, human beings have to go through variety of technological devices or mediums such as social networks, ATM, CCTV cameras, biometric identifications and much more to perform their everyday activities. All these mediums somehow the other way give birth to function creep and have put the privacy on stake. Based on the concept of function creep in surveillance techniques the following data has been collected to get the views of the general public.

B. Survey Results Analysis

Data has been collected from different departments' e.g. educational institutes, police department, NADRA and banking sectors to get into a precise conclusion. Based on the collected data it has been concluded that CCTV cameras, ATM, biometric devices and social networks are used by everyone on daily basis. Most of them are unaware of facial recognition system, but they agree to the point that collecting data about a particular person without his/her knowledge is the violation of basic human rights. No one denies the pros of surveillance techniques but there must be some surety that it will not create many problems than it solves. The following questions were asked during the survey.

Q1. Have you ever provided Biometric identification for gettingaservice?

Q2. Based on other researches, "Function Creep causes innocent people categorized in wrong and dangerous groups", would you allow this to happen if it were in your knowledge?

Q3. Do you know about Facial Recognition Systems?

Q4. Based on other researches, “Watch the Watchers” technique can reduce the happenings of function creep in surveillance techniques, would you support this solution if properly implemented?

Q5. Do you agree that strong actions should be taken to control and regulate the use of surveillance techniques for protecting our basic human rights?

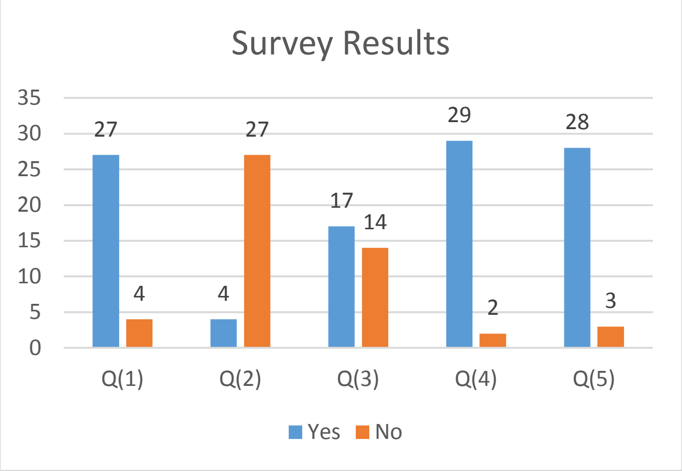

Figure 1. Comparative result of survey

People want strong actions or a governing body to protect their basic human rights. They also agree to the point that “watch the watchers” technique can lessen the happenings of function creep in surveillance techniques if and only if implemented properly. Moreover, people should be given the right to all the information collected about them to make better use of these advanced techniques.

IV. CONCLUSION

No one will ever deny the benefits of surveillance practices as it depicts a reassuring image that if something bad happens there will be information stored in different formats giving a sense of protection to the general public. However, very few people know about the risks and threats attached to these practices. The biggest problem of the latest surveillance practices and tools is only benefits are conveyed to the public but the negative effects and threats are rarely addressed. People are unaware of the fact that they are enjoying security by paying a huge amount in return. Function creep is a term, which mainly grows gradually and subtly with time, particularly, in surveillance rehearses and empowers these practices to be utilized for new and/or different capacities, which either nobody knew before or were unintended at the outset however even exceptionally, few of its affectees think about it after it happens. Facial recognition system and biometrics are some of the commonly used security systems and are known as the best protection means but, there should be some obligations and limitations while using the information collected for security reasons. Moreover, if there is a need to share an individual’s information s/he should be informed beforehand. It is noted that Function creep damages the privacy rights to a significant level and have given birth to intentional isolation and segregation of various social groups.

V. REFERENCES

[1] Alterman, A. (2003). ‘``A piece of yourself'': Ethical issues in biometric identification', Ethics and Information Technology, vol. 5, no. 3, pp. 139-150.

[2] M. A. Jan, P. Nanda and X. He, “Energy Evaluation Model for an Improved Centralized Clustering Hierarchical Algorithm in WSN,” in Wired/Wireless Internet Communication, Lecture Notes in Computer Science, pp. 154–167, Springer, Berlin, Germany, 2013.

[3] M. A. Jan, P. Nanda, X. He and R. P. Liu, “Enhancing lifetime and quality of data in cluster-based hierarchical routing protocol for wireless sensor network”, 2013 IEEE International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing (HPCC & EUC), pp. 1400-1407, 2013.

[4] M. A. Jan, P. Nanda, X. He and R. P. Liu, “PASCCC: Priority-based application-specific congestion control clustering protocol” Computer Networks, Vol. 74, PP-92-102, 2014.

[5] Fox, R. (2001) 'Someone to Watch Over Us:: Back to the Panopticon?', Criminology and Criminal Justice, vol. 1, no. 3, pp. 251-276.

[6] Van, L. & L, Royakkers. (2004) 'Ethical issues in web data mining', Ethics and Information Technology, vol. 6, no. 2, pp. 129-140.

[7] Mian Ahmad Jan and Muhammad Khan, “A Survey of Cluster-based Hierarchical Routing Protocols”, in IRACST–International Journal of

Computer Networks and Wireless Communications (IJCNWC), Vol.3, April. 2013, pp.138-143.

[8] Mian Ahmad Jan and Muhammad Khan, “Denial of Service Attacks and Their Countermeasures in WSN”, in IRACST–International Journal of Computer Networks and Wireless Communications (IJCNWC), Vol.3, April. 2013.

[9] M. A. Jan, P. Nanda, X. He and R. P. Liu, “A Sybil Attack Detection Scheme for a Centralized Clustering-based Hierarchical Network” in Trustcom/BigDataSE/ISPA, Vol.1, PP-318-325, 2015, IEEE.

[10] Wright, D., Friedewald, M., Gutwirth, S., Langheinrich, M., Mordini, E., Bellanova, R., De Hert, P., Wadhwa, K., & Bigo, D., (2010)'Sorting out smart surveillance', Computer Law & Security Review, vol. 26, no. 4, pp. 343-354.

[11] Hough, M., (2009) 'Keeping it to ourselves: Technology, privacy, and the loss of reserve', Technology in Society, vol. 31, no. 4, pp. 406-413.

[12] Elahi, S. (2009) 'Privacy and consent in the digital era', Information Security Technical Report, vol. 14, no. 3, pp. 113-118.

[13] Schneier, B. (2010) 'Security and Function Creep', IEEE Security & Privacy Magazine, vol. 8, no. 1, pp. 88-88.

[14] Levi, M. & Wall, D. (2004)'Technologies, Security, and Privacy in the Post-9/11 European Information Society', Journal of Law and Society, vol. 31, no. 2, pp.

[15] M. A. Jan, P. Nanda, X. He, Z. Tan and R. P. Liu, “A robust authentication scheme for observing resources in the internet of things environment” in 13th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 205-211, 2014, IEEE.

[16] M. A. Jan, “Energy-efficient routing and secure communication in wireless sensor networks,” Ph.D. dissertation, 2016.

[17] Donahue, J., Whittemore, N., and Heerman, A. Ethical Issues of Data Surveillance.EthicaPublishing http://www. ethicapublishing.com/ethical/3CH20. pdf.

[18] Lockton, V. & Rosenberg, R. 'Technologies of surveillance: Evolution and Future Impact'. [Online]. http://www.ccsr.cse.dmu.ac.uk/conferences/ethicomp/ethicomp2005/abstracts/71.html

[19] Carrigan, M. & Kirkup, M. (2000)Video surveillance research in retailing: ethical issues. International Journal of Retail & Distribution Management, 28 (11), 470-480.

[20] Clarke, R. (2001). Roger Clarke’s ‘Biometrics and Privacy’. [Online]. Available: http://www.rogerclarke.com/DV/Biometrics.html.

[21] Smith, T. (2013) “The Impact of Biometrics,” Ph.D dissertation, Dept. Comput. and Elect. Syst., Ohio Univ., Ohio, United States.

[22] Levi, M. & Wall, D.S. (2008) “Technologies, Security and Privacy” Journal of Law and Society, vol. 31, no. 2, pp. 194-220.

[23] Watch, G. (2006). Using the Police National DNA Database - under adequate control? [Online].Available:http://www.genewatch.org/uploads/f03c6d66a9b354535738483c1c3d49e4/research_brief_fin.doc.

[24] Gayton, C. M. (2006)Beyond terrorism: data collection and responsibility for privacy. VINE, 36 (4), 377-394.