Surveillance Threatening Privacy and Data Protection: A Review

Sheshadri Chatterjee

Indian Institute of Technology, Hauz Khas, New Delhi, India
E-mail: sheshadri.academic@gmail.com

Received 2018-02-01; Accepted 2018-02-26
DOI: http://currentsciences.info/10.15520/ctst.v8i03.360.pdf

ABSTRACT:
To combat crime and terrorism there is necessity of surveillance. The word “surveillance” originates from French verb, “Surveillar”, which means “To watch over”. Modern surveillance technologies named as Smart Surveillance are being deployed almost everywhere and it is sadly observed that surveillance used for various purposes is also posing threat to privacy and data protection. To combat crime and terrorism, use of smart surveillance should not be so applied that it becomes cause to dishonor privacy and personal data protection. This paper has taken a sincere attempt to review different surveillance techniques and related privacy challenges affecting the society.

Keywords: Legislation; Privacy; Security, Surveillance; Terrorism

I. INTRODUCTION:
It is a fact that in previous days surveillance technologies were used as a monopoly by intelligence agencies or by military to combat crime or to put border areas calm and quiet. But now-a-days situation has become otherwise. Modern information technology is using surveillance processes in everyday life. It is being used in central traffic activities, employers with the help of surveillance activities are found monitoring their employees especially for their unnecessary use of internet, for their overuse of office phones for their personal grounds, parents are found using surveillance processes to monitor their children’s whereabouts, fingerprints are being stored to keep records of arrival and departure of the employees etc. Thus, we find that surveillance has entered our daily life without even our notice. Use of surveillance has become a routine matter in our everyday life. Previously we knew that surveillance is done through cameras (CCTV), but now other surveillance technologies like Radio Frequency Identification, Biometrics etc. are being frequently deployed. Information reveals that people in London are captured by CCTV cameras almost 400 times a day. Now data are being used to surveil and monitor citizens [1]. In some cases, it appears that some specific applications of surveillance activities are being supported by the citizens but some of the applications are also not being supported by the citizens though they know their protest this would
not fetch any result [2]. This phenomenon is called “Cognitive Discordance”. Now the surveillance activities are not only used for security purposes but also, they are used for different necessities as a routine use [3]. This paper will deal with modern surveillance technologies befitting with the demand of the day. However, this modern surveillance processes known as “Smart Technology” is required to be sorted out meticulously so that its frequent use may not jeopardize security and privacy issue. Here we will deal with the fact that whether such legal tool is available which can cordially respect the security, privacy and data protection issues. We also would examine what improvements may be made so that proper honor and respect may be given to the issues of the society which may not be at stake at the expense of “Smart Surveillance”.

II. DEFINITION OF SURVEILLANCE:

It is a fact that many researchers and experts in this field have conceptualized “Surveillance” in different perspectives. Surveillance refers to “close watch kept over someone or something” [4]. In another angle, surveillance refers to “the process of watching, monitoring, and processing the behavior of people, objects and events to govern activity [5]. A question is very relevant and important to be dealt with: “How one can conceptualize surveillance?” In this context Michel Foucault provided a model named, “discrepancy model” where it is found to have been illustrated by “panopticon” which means “inspection house”. “Panopticon” is nothing but it is a principal of construction of model which is a circular building having a central observatory wherefrom activities at the parameter may be observed. Here those who are in the periphery cannot see their observers, but they assume that they are being carefully watched by someone. Practically “panopticon” is a construction model which aims “to reduce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power” [6]. “Panopticon” is a constructional conception which ensures control and discipline. This example gives much stress on supervision and less stress on surveillance and collection of information and data [7]. Thus, it is noticed that idea of surveillance has extended its amplitude and now it does not only mean keeping watch over prisoners or over unfortunates, but it is now covering so many social behaviors.

III. UNIVERSAL USE OF SURVEILLANCE

It is noteworthy to state that in all developed and developing countries there is a tendency that all the cities therein are required to be globalized cities e.g. in China there are so many cities by this time are intending to relish the complexion of globalized cities and by this time there has been extensive studies on China’s globalization and urban change [8, 9, 10, 11, 12, 13, 14, 15]. Naturally if all cities are globalized, the deployments of surveillance technologies will play a very prominent role. Nowadays anyone thinks that he is living in a society of surveillance, he must not think that he is living continuously under careful watch of CCTV cameras because in modern world movement of every citizen is constantly being digitalized [16]. Even digitalized specialties of human body, internet and intelligence techniques are being frequently used. This has developed a sense of connected world including access of public security organizations which can directly affect the personal life [17]. It is a bare fact that with time, population is increasing out of proportion in every city. As a result, streets are being overcrowded and hence to keep security intact, surveillance through CCTV cameras has become a dire necessity [18]. Surveillance has become a daily affair in the society and it bridges a good relationship indirectly between individuals and the state and even it has established tie of relation in between individuals and individuals [19]. In modern world, there is no denying the fact that privacy is essential to exercise freedom of individuals and if it is eroded, it would eventually weaken the plinth of constructional foundation of a country on which good governance is based. It is admitted that for detecting any breach, process of surveillance in any congenial form is necessary but recently unfortunately its frequent and uncontrolled applications have become a subject of great concern to the privacy experts. In International Conference of Privacy and Data Protection Commissioners held on November 2009 at Madrid there was a declaration: “Global Privacy Standard for a Global World” which practically noted that, “the dramatic expansion of secret and uncountable surveillance, as well as growing collaboration between Governments and Vendors of surveillance technology has established a new form of social control.” In that conference, a warning was given as “that privacy law and privacy institutions have failed to take full account of new surveillance
practices including behavioral targeting, data bases of DNA and biometric identifiers, the fusion of data between the public and the private sectors and the risks of vulnerable groups, including children, migrants, and minorities” [20]. Ironically, the use of surveillance has become so much in the societies particularly in cities that it has raised serious concerns of individuals, different organizations, media and even of the policy makers [21]. Now city authorities have started using surveillance technologies even to spy on household families to control flimsy sort of so-called offences including littering, allowing pet dogs to foul the pavements etc. [22]. Practically this kind of surveillance is too much, and this unreasonable strictness has adverse adumbration on the freedom [23]. The discussions above including mentioning of series of instances highlight that at least time has come to think sincerely that a device in the form of appropriate mechanism is essential to control the over use of surveillance technology which is sometimes directly and sometimes indirectly jeopardizing the high respect of privacy and freedom.

IV. SMART SURVEILLANCE TECHNOLOGY AND PRIVACY:

Here we shall discuss how modern surveillance technologies are shadowing impact on social behavior and to what extent these technologies are honoring privacy and are protecting menace of data disclosure. There are three major changes in surveillance technology which are highly and adversely affecting the society. These are New Image Analysis Technique [24, 25], New Sensor System and New Data Integration Effort. These three dimensions have been illustrated through three figures.

V. SURVEILLANCE AND SOCIO-POLITICAL PERSPECTIVE:

Over use of surveillance technologies are posing threat to privacy [26, 27]. From long time, back process of surveillance has been misused threats privacy [28, 29, 30]. From an I.B report in India it has come to the public that from 1948 to 1968 surveillance has been constantly made over the movement of Netaji Subhas Chandra Bose, a great freedom fighter of India and knowing this there has been a great turmoil in the political atmosphere of India inculpating the then ruling party of India since they took this heinous initiative for the surveillance at the cost of privacy of this great freedom fighter of India [31] and hence it is not a new thing that misuse of surveillance technologies cast adverse shadow even over the privacy of individual.
it has been for a long time felt essential to establish a balance between surveillance and respect of privacy [32]. It is a fact that sad incidence of 9/11 brought a radical change of geo-strategic scenario and as a result keeping that in view a challenge to combat international terrorism was recognized in December 2003 in Europe and a security strategy was adopted: “A secure Europe in a better World” [33] and the European Authority felt the need of ensuring safeguard and security of its citizens and it was felt that, “Europe must take advantage of its technological strengths” to achieve the goal [34]. In one hand, it is felt that to ensure security and to combat threat of terrorism the importance of applications of surveillance technologies cannot be set at naught but on the other hand ceaseless misuse of surveillance technologies even today is posing ruthless threat to privacy. In India, during first week of April 2015 in Goa (A south western state of India) Minister-in-Charge, Human Resource and Development, Smriti Irani for purchase of some personal garments went to a shop and while she was attempting to dress her with the new garment for checking its fitness in the trial room of the shop, viz, “Fab India Ltd.” she noticed that her such activities are being covered by one CCTV camera installed in the trial room endangering thereby the privacy of a woman. Thus, it is seen that at the cost of security, privacy of a woman even is at stake [35]. Something really is to be done to keep this in check. Again, this is also a matter of great concern that data collected for one purpose is used for another purpose, e.g. in the year 2006 at Graperine in Law Enforcement Information Management Conference, the presenters of IBM on the topic, “Smart Surveillance Solution” stated, “There is a lot of video captured and stored and often the value of the video is unknown well after time of capture. Stored video is potentially valuable latter” [36]. This indicates that even the technologists are aware of the negative social effect of surveillance technology.

VI. PRIVACY, DATA COLLECTION AND LEGAL ISSUES:

It is a fact that in every country applications of surveillance technology influence the society either in the right way or in a wrong way. As such there also exists legal protections against those applications of surveillance which bring in bad effects or threats to the privacy issues of the society. The legal protections create a bar so that such applications of surveillance may not jeopardize the sense of privacy. But since as the days roll on greater is the frequency of applications of “Smart Surveillance” and as such to combat this threat of jeopardizing the privacy and data protection with time, the age-old legislation protecting these are required to be galvanized and amended befitting with the demand of the situation. In Europe instances are not rear where to ensure protection of privacy at the threat of “Smart Surveillance” there were many court cases and case laws which offer also some important guidelines [37, 38]. In different countries for ensuring different protective measures against privacy issues and issues connected with personal data protection, some enactments have been made. In India through Cyber Laws such protections have been given. However, these all enactments are accepted to be not so strong to put a complete full stop in this issue and as such the privacy experts and Governments of developed and developing countries are profoundly thinking to improve their laws to make it more stringent. It is also experienced that the Governments of developed and developing countries where there are extensive applications of “Smart Surveillance” techniques are found to be more serious to cope up with the menace of security and terrorism issues compared to their seriousness regarding actions to be taken to safeguard and protect privacy and data hijacking. Privacy may be at stake but never the security. It is the common doctrine everywhere. However, as it has already been mentioned that case laws connecting protection of privacy and data protection gave some guidelines to different countries but in United Kingdom, ironically, it is noticed that despite court judgement the concerned Government is found to be reluctant to comply with court’s order [39] presumably apprehending that such compliance might endanger the security issue.

VII. PRIVACY IMPACT ASSESSMENT:

Privacy Impact Assessment (PIA) is a very important tool for safeguarding different types of privacy e.g. privacy by design, privacy certification scheme [40], best available practices and privacy standards [41]. PIAs provide a tool for introducing more trust using personal data. It may be taken as an important tool for risk management. PIAs have been defined in many ways by different experts basing on presumably different perspectives. However, PIA may be conceptualizing as “a
systematic process for evaluating the potential effects on privacy of project, initiative of proposed system or scheme and finding ways to mitigate or avoid any adverse effect” [42]. PIA is associated with a belated assessment of public reaction against the privacy-harmful actions of Governments and Corporations. This PIA methodology imports a very good mechanism which helps the stakeholders to assess the impacts and issues cropping up owing to continuous deployment of “Smart Surveillance” technology and to consider alternatives to mitigate adverse effect of smart technology. In respect of use of CCTV cameras famous expert Introna and Wood commented, “Seemingly mundane design decisions may have important political consequences that ought to be subject of security” [43]. PIA is nothing but an incubation of rational management technique. Governments of different developed and developing countries have featured PIA as a risk management to respect the privacy and personal data protection [44]. So many countries like Australia, Canada, Hong Kong, New Zealand, the UK and USA are using this PIA technique to mitigate adverse effect of privacy [45]. The existing methodology focuses mainly on data protection rather than on protecting privacy. This deficiency requires improvement. PIA technique is required to be restructured in such a fashion as it can deal with surveillance involving law enforcing activities. It is proposed that PIA methodology should cover prohibitive as well as regulatory aspects of surveillance projects [46]. When the privacy is at stake, the outcome of PIA should be simply “no” to the proposed technique. Attempts are scheduled to be taken to restructure the PIA technique in such a fashion as it can cover all the surveillance issues.

VIII. CONCLUSION AND CHALLENGES AHEAD:

It has been observed that reckless use of surveillance technologies is jeopardizing the privacy and personal data protection. As has been discussed it is seen that to combat this, a technology known as PIA is used. But it also has been experienced that this methodology is not capable of covering all the angles. Cross border terrorism is increasing. To check this, new technique of surveillance is used. Such use of new technique is putting plug on terrorism activities but at the same time such application of surveillance technology connected with combating cross border terrorism is hatching new menace to the privacy since it cannot be kept in check through PIA technique as this PIA technique has yet not been internationalized. It is proposed that attention to be given to this point. It is also concluded that PIA should be structured, in addition, to cover privacy of personal information, privacy of persons and privacy of personal communications. In this way PIA might emerge as a strong tool to address privacy too. As has been noted that the enactments already in existence in different countries in favor of privacy and data protection are not very strong nor they appear to cover all the corners. Hence there are still some challenges left unsolved and it is proposed that future researchers would strive to address those challenges. And the challenges are:

i. If frequency of security check and surveillance are combined and if national and international securities are combined, how principles of privacy and data protections would be applied?

ii. How modern technologies like data mining and data profiling posing threat to data protection could be checked and regulated?

iii. It is a fact that data of commercial and non-commercial nature are constantly processed for surveillance and security purposes. What should be the relevant framework of privacy and data protection and what will be the technique of applying that framework?

iv. Some data might be relevant for a wide range of state activities and law enforcement and if these data relate to non-identified persons then what will be the legal protection for those data?

REFERENCES:


17. Taken from http://www.edps.europa.eu/EDPSWEB


32. Available at EC.COM (2004), 590 final, op.cit.


40. Taken from www.european-privacy-seal.eu/


45. Protection of individuals about the processing of personal data by community institutions and bodies and the free movement of such data, Regulation [EC], No. 45/2001, 18, December 2000.