ISBN 978-93-5156-328-0
International Conference of Advance Research and Innovation (ICARI-2014)

A study on Electronic surveillance

Vivek Sharma [a,*], Anshu [b,*]
[a] Department of Computer Science and Engineering, Shri Venketeshvara University, Gajraula, U. P, India
[b] Department of Computer Science and Engineering, TMU, Moradabad, Uttar Pradesh, India

Article Info

Article history:
Received 2 January 2014
Received in revised form
10 January 2014
Accepted 20 January 2014
Available online 1 February 2014

Keywords

Abstract

Surveillance is the monitoring of the behaviour, activities, or other changing information, usually of people for the purpose of influencing, managing, directing, or protecting. Surveillance is therefore an ambiguous practice, sometimes creating positive effects, at other times negative. It is sometimes done in a surreptitious manner. It most usually involves observation of individuals or groups by government organizations. The purpose of this paper is to explore Electronic surveillance.In the last 20 years, there has been a virtual revolution in the technology relevant to electronicSurveillance. Advances in electronics, semiconductors, computers, imaging, data bases, and related technologies have greatly increased the technical options for surveillance activities. Closed circuit television, electronic beepers and sensors, and advanced pen registers are being used to monitor many aspects of individual behaviour. Additionally, new electronic technologies in use by individuals, suchAs cordless phones, electronic mail, and pagers, can be easily monitored for investigative, competitive, or personal reasons. This topic is also an important informant to my work as an artist in the field of new media as it seeks to examine the art and technology of surveillance and its existence in today's society as a system that we are able to employ for our own benefits and security. Current R&D will produce devices with increased surveillance capabilities, e.g., computer speech recognition and speaker identification, fibre optics, and expert systems many electronic devices are currently available for monitoring individual or group behaviour. New surveillance tools are technically more difficult to detect, of higher reliability and sensitivity, speedier in processing time, less costly, more flexible and adaptable, and easier to conceal because of miniaturization and remote control.

1. Introduction

Electronic surveillance is the epitome of the two-edged sword of technology for everyone. Polls by Public opinion evidence considerable concern about possible excessive and abusive use of electronic surveillance by the Government (and others), and show support for strong safeguards and protections to tightly control the use of such technology. But, at the same time, the public is concerned about crime—especially violent crime—and supports the appropriate use of technology to combat and prevent crime and bring offenders to justice. ' Until the past 10 years or so, the balancing of these concerns was relatively straightforward from a technological perspective.

Corresponding Author,
E-mail address: anshu_27aug@yahoo.co.in

Now, however, technological developments have significantly expanded the range of electronic surveillance options. These include miniaturized transmitters for audio surveillance, lightweight compact television cameras for video surveillance, improved night vision cameras and viewing devices, and a rapidly growing array of computer-based surveillance techniques. In addition, most forms of electronic communication—whether via wire, coaxial cable, microwave, satellite, or even fibre optics—can be monitored if one has the time, money, and technical expertise. The primary purpose of electronic surveillances to monitor the behavior of individuals, including individual movements, actions, communications, emotions, and/or various combinations thereof, as well as the movement of property or objects.

However, while providing increased security, the use of sophisticated technologies for surveillance a purpose also presents possible dangers to society.'

Over time, the cumulative effect of widespread surveillance for law enforcement, intelligence, or other investigatory purposes could change the climate and fabric of society in fundamental ways.

2. History

For much of the 20th century, electronic surveillance technology was limited primarily to audio surveillance devices such as telephone taps and concealed microphones ("bugs"). In the late 1960s, however, technological developments began to significantly expand the range of electronic surveillance options. These included miniaturized transmitters for audio surveillance, lightweight compact television

Cameras for video surveillance, improved night vision cameras and viewing devices, and the first computer-based surveillance techniques. In the 1970s, congressional attention focused on electronic surveillance, partly due to the use of surveillance technologies during the Civil Rights Movement and in Watergate, but also due to a perception of a growing application of such technology in various sectors of society. It appears that many of the electronic surveillance technologies identified were not widely used in 1976, partly because the underlying media of communication were not in wide service. However, there is no authoritative information on the full extent of their use.

3. Types of electronic surveillance

1. Telephone Surveillance
2. Electronic Mail Surveillance
3. Electronic Physical Surveillance
4. Electronic Visual Surveillance.
5. Data Base Surveillance

3.1 Telephone Surveillance

The public generally expects that telephone conversations are private, and that electronic surveillance of telephone calls (sometimes known as wiretapping or eavesdropping) is illegal, except in very narrowly circumscribed law enforcement and national security investigations. But technological innovations now make it easier to electronically monitor both the content of phone calls and phone transactions. Furthermore, the new telephone technology was not envisioned when current legal protections were enacted, and thus the statutory protection against telephone surveillance is weak, ambiguous, or non-existent. Most phone users have assumed high degree of confidentiality for their phone calls. This has been especially true as private lines and improved connections replaced party lines and broken connections. In some respects, the technology has brought more assurances for the protection of the privacy of phone calls than did the law. However, this is now changing. Four technological innovations in phone service—digital transmission, new types of phones, new phone networks, and the ability to easily collect detailed information on phone usage—make it easier both to overhear the content of phone calls and also to monitor phone transactions.

With the conventional telephone, phone calls were transmitted in analog form across wire lines. Today, an increasing percentage of phone calls are converted from analog to digital form and then transmitted. Transmission may be over wire, but is often via microwave radio and satellite systems and, increasingly, via fibre optic transmission facilities.

Additionally, new phones are making use, in whole or in part, of radio communications. Cellular or mobile phones use radio to transmit messages between a phone and a switching centre, while cordless phones use radio to carry messages between the phone base station and the cordless phone handset. Another growing gap in the protection afforded phone calls is between common carrier calls and private network calls. Thus, the privacy of the content of digitized phone calls, cellular and cordless phone calls, and private carrier calls may not be afforded protection against interception by either Government officials or private parties. Moreover, technological changes make it far easier today to monitor phone transactions. Pen registers are devices by which Government officials or private parties can monitor the numbers dialed on a given line. Increasingly, computerized telecommunications switching equipment can collect and store information on the numbers dialed and length of phone calls. This information may be kept for billing and administrative purposes, but it also has monitoring capabilities. As automatic call accounting becomes widespread, pen registers will become unnecessary.

3.2 Electronic Mail Surveillance

The public expects and is provided with a high standard of protection against unauthorized opening of first-class letter mail when in paper form and delivered by the U.S. Postal Service. Constitutional provisions, case law, and postal statutes and regulations collectively provide such protection. However, when mail is sent in electronic form, the existing protections are weak, ambiguous, or non-existent. Electronic mail is a relatively recent marriage of computer and communications technology that makes it possible to send, transmit, and receive mail in electronic form. If desired, the electronic output can be printed out in hardcopy and delivered by the USPS or private carrier. But

electronic mail also permits terminal-to-terminal communication where the message is never in paper form. Various private companies now offer electronic mail services. The interception of electronic mail at any stage involves a high level of intrusiveness and significant threat to civil liberties. The investigative value of intercepting electronic mail will vary. But, traditionally, paper mail has been afforded a high level of protection from interception.

3.3 Electronic Physical Surveillance

Maintaining physical surveillance of individuals is, traditionally, one of the most expensive and risky surveillance techniques used bylaw enforcement agencies and others. Portable telecommunications devices are now offering viable substitute in many cases. For example, electronic beepers emit a radio signal that can be monitored in order to track the movements of a car or piece of property to which a beeper is attached. Also, electronic pagers—increasingly used by busy executives, repair personnel, doctors, and the like-can be intercepted to reveal information that may be useful in determining the subject's location and activity. Based on criteria used to determine the threat to civil liberties-nature of information, nature of place or communication, scope of surveillance, surreptitiousness of surveillance, and pre-electronic analogy-electronic physical surveillance appears to fall somewhere in the middle. The investigative and law enforcement interest appears to be significant-especially for beepers.

In the past, physical surveillance has generally required around-the-clock agents with backups at various points and has entailed a high risk of detection by the party under surveillance. Monitoring by portable telecommunications devices, or tracking devices, provides a much less conspicuous way of following the physical activities of an individual, a car, or an item, Monitoring by portable telecommunications devices is relatively risk-free in terms of detection. Physical surveillance can be more efficient with the use of portable telecommunications devices. However, electronic tracking may cost more because surveillance can be carried out for a longer period and because of the staff necessary to monitor the information received. The availability of new electronic physical surveillance devices to law enforcement agencies is likely to have significant effects on the investigative process. Before the invention of such devices, it was generally assumed that an individual who was engaged in illegal activity was suspicious and was, therefore, aware that someone might be watching.

3.4 Electronic Visual Surveillance

Electronic visual surveillance through the use of cameras is an alternative to physical surveillance. In the past, however, the size, cost, and technical requirements of cameras have limited their effectiveness and usefulness. But the latest generation of cameras is smaller, cheaper, and easier to operate. There already is a significant level of video surveillance of public places, such as the use of closed circuit TV in banks, building lobbies, retail stores, and the like. In addition, video surveillance of private places is used for investigative and law enforcement purposes.

Electronic visual surveillance appears to pose a substantial threat to civil liberties, especially if conducted in private places and with audio surveillance. The law enforcement interest varies depending on the stage of investigation. As cameras have become smaller and easier to activate from a distance, they have become more attractive as a tool for watching people and recording their activities. The evidence that can be obtained from electronic visual surveillance, especially if accompanied by audio surveillance is as complete as investigative authorities could expect. But there are questions about the intrusive nature of electronic visual surveillance, and the circumstances under which its use is appropriate.

There is presently a great deal of electronic visual surveillance of public places. Banks have cameras running continuously to monitor both the interior teller counters and also the outside automatic teller machine areas. Airports use electronic visual surveillance in a number of places to ensure the security of the passengers and equipment. Many large department stores, as well as all-night convenience stores, use electronic visual surveillance to deter and detect shoplifting and to compile a visual record of activity. Many cities use closed circuit television to survey street corners in high crime areas, subway platforms, and entrances to public buildings. Some employers, especially factory owners and those who maintain large clerical pools, use electronic visual surveillance to monitor the activities of workers. The motivation for this electronic visual surveillance is a heightened concern for security; the result is that people are becoming more and more accustomed to being watched as they carry out their public life. As cameras become smaller, and easier to install and to monitor, their attractiveness as a means of monitoring activities in private places becomes greater. Previously, one could take actions to ensure an expectation of privacy in a private place.

3.5 Data Base Surveillance

As computerized record systems and data communication linkages become widespread, the potential for computer-based surveillance of the

movements and activities of individuals also increases. Various investigating agencies already maintain computerized record systems that could be used as part of a data base surveillance network.

Investigating agencies believe that these and other systems are essential to carrying out their authorized responsibilities. However, the systems could include files on any definable category or type of persons, and could be interconnected with numerous other computerized systems.

A significant implication of widespread computerized record systems and data communication linkages is the increased potential for computer-based surveillance of the movements and activities of individuals. In modern society, most persons leave a trail of transactions with various institutions governmental, retail, financial, educational, professional, criminal justice, and others.

In theory, the technology permits the instantaneous linkage of a large number of record systems that would capture and consolidate. Thus, electronic linkages could be used to conduct surveillance of individuals who are of investigative, law enforcement, and/or intelligence interest to the Government. This assumes, of course, that the Government agencies would have electronic access to transactional record information.

4. Challenges & Issues

4.1 Resource constraints

Electronic evidence gathering is necessarily a costly endeavor. It requires technology adequate to undertake the surveillance, which must be frequently updated to ensure that it remains effective. Additionally it requires sufficient manpower to not only undertake the surveillance or interception but also to process the information obtained. Often the material collected is in significant quantities and might take several officers a very lengthy period to disseminate. Thus the strain on resources is significant and may discourage investigative agencies and law enforcement from conducting such investigations.

4.2 Training

In the 2009 expert group meeting some participants emphasized that lack of specialist training for law enforcement significantly hindered their capacity to engage in electronic evidence gathering to any significant degree. Moreover, prosecutors and judges are not always aware of the latest technological advances for the conduct of electronic surveillance. Training in the laws, regulations and operative procedures for conducting overt electronic surveillance should be mandatory for investigative officers involved in managing such techniques. Training is recommended also for other officials such as prosecutors and judges who will be involved in cases where such evidence is or may be used.

4.3 Technological challenges

Inevitably regulation will always be playing catch-up with technological developments. And is not always the case that the technological advancements are in the hands of the investigators before they are in the hands of criminals. Resource constraints in particular limit the attainment and thus use of hi-tech surveillance equipment and technologies by investigating authorities. Some of the current technological challenges faced by law enforcement and investigators in pursuing electronic evidence gathering were discussed in the expert group meetings, particular that which took place in 2007.

Some of the issues raised are listed below and they highlight the increasing complexity of such investigations.

- **Telephone number portability and roaming:** Telephone number portability means that consumers can change telecommunication service providers (TSPs) without changing their phone number. In addition, mobile phones can roam different TSP networks. This can make it difficult for investigators to identify which service provider through which to intercept communications and this in turn can cause delay to investigations and thus risk failing to obtain important evidence.
- **Email, chat and voice over internet protocol (VOIP):** Email, chat and VOIP present unique technical and legal challenges. VOIP interception allows monitoring to occur in real-time. However, this risks the inadvertent recording or monitoring of material which could be legally privileged. If the material is privileged it is not only likely to be inadmissible as evidence but it could throw into question the other evidence gathered in the investigation by the same technique. Interception or monitoring of computer information is also complicated by the suspect's use of wireless internet hot spots in places such as cafes, airports and other areas where free wireless internet services are available. A range of privacy protection and virus protection software is now available to consumers. Because the software is designed to protect personal computers from attack, the software can interfere with computer-based electronic evidence gathering.
- **Telecommunications service providers:** Telecommunications service providers (TSPs) play an important role in enabling the interception of communications. Participants in the initial expert group meeting suggested that Although TSPs are generally cooperative, there have been instances

where they have been reluctant to comply when there is no actual or perceived commercial advantage in doing so. Some countries have dealt with this by enacting legislation which not only requires TSPs to ensure that their networks are compatible with interception requirements of police but also that any request for assistance by law enforcement or the relevant authority is complied with, regardless of the cost.

- **Tracking:** Tracking devices throw up another set of technological challenges. These devices are quite heavily power dependant and thus their use can be limited to that which their power source (often batteries) can sustain. Similarly, when tracking a suspect using the built-in GPS in a mobile phone, pulling the location drains the battery of the mobile phone. When regulating for tracking devices it is important that legislators bear in mind not only the use of tracking devices which can be covertly installed into or onto objects by authorities but also the use of technology which already exists in objects such as GPS in cars and mobile-phones. That is, any system of authorization should anticipate the use by law enforcement of tracking devices already existent in the suspect's possession.

5. Importance of Electronic Surveillance

There are varieties of processes to the people all around the globe. Wiretapping is the oldest means of examination used in the telephone communications and still being utilized in most of the government, military and law enforcements units. But in the present preview, role of wiretapping has been limited since these processes cannot be conducted without the prior permission of the government. Another kind of examination practice is bugging where small microphone and chip is installed to get the details of the conversations between partners in the noisy and crowded areas. Latest processes is video surveillance which are used by international police and law enforcement agencies to monitor, identify and nab the criminal before they commit any harm to the community. These processes are recorded as the evidence preserved for the trial in the courts. Any kind of suspicious and sabotages activity are completely covered through such processes.

The demand for the electronic surveillance of the employees is rising annually as per the electronic monitoring conducted by the many organizations. These are the provisions to monitor the activities of the employees in major shopping malls, high ways, sidewalks, retail stores and corporate offices. There is the excessive need to protect the assets and properties. Risks to the assets, properties and danger at the crowded area are felt more due to existing threats in the existing society. Shopliftings sabotage and vehicle thefts are serious criminal activities which are required to be monitored through such processes. Besides, there are cases of the misuse of emails and internet by the employees and deteriorating the working environment of the corporate. These activities are spoiling the healthy atmosphere of the corporate and had been providing the higher risks. Corporate are analysing these risks and feeling the huge need of right actions to deter the rise of such risks with effective monitoring of their employees.

6. Conclusion

This reveals that the electronic surveillances are the useful and beneficial process to protect the installations, monitor and regulate the crimes by adequate law enforcements. The purpose of this paper is to argue that it is important to deal with the theoretical question of how surveillance can be defined. Surveillance is a specific kind of information gathering, storage, processing, assessment, and use that involves potential or actual harm, coercion, violence, metric power relations, control, manipulation, domination, disciplinary power. It is instrumental and a means for trying to derive and accumulate benefits for certain groups or individuals at the expense of other groups or individuals. Surveillance is based on logic of competition. It tries to bring about or prevent certain behaviors of groups or individuals by gathering, storing, processing, diffusing, assessing, and using data about humans so that potential or actual physical, ideological, or structural violence can be directed against humans in order to influence their behavior. This influence is brought about by coercive means and brings benefits to certain groups at the expense of others. Surveillance is in my view therefore never co-operative and solitary – it never benefits all.

References

[1] Ainne Basant, Importance of Electronic Surveillance, http://goarticles.com/article/Importance-of-Electronic-Surveillance/7213201/
[2] Mark D. Young , Cyber security and the United States Congress, www.csfi.us/pubdocs/?id=11
[3] Dr. C. Michael Walton, Electronic Vehicle Identification: Industry Standards, Performance, and Privacy Issues, 2007
[4] Federal Government Information Technology: Electronic Surveillance and Civil Liberties

[5] (Washington, DC: U.S. Congress, Office of Technology Assessment, OTACIT-293, 1985
[6] (Washington, DC: U.S. Congress, Office of Technology Assessment, OTACIT-293, 1985
[7] Electronic surveillance in an era of modern technology and evolving threats to national security. http://www.thefreelibrary.com/ Electronic+surveillance+in+an+era+of+modern+technology+and+evolving...-a0261729763
[8] Daniel J. Solove, Reconstructing Electronic Surveillance Law, 73 GEO. WASH. L. REV. 1264, 1266, 2004
[9] Daniel T. Keuhl, From Cyberspace to Cyber power: Defining the Problem, in CYBERPOWER AND NATIONAL SECURITY 24-31 (Franklin D. Kramer, Stuart H. Starr & Larry K. Wentz eds., 2009
[10] Current practices in electronic surveillance in the investigation of serious and organized crime, UNITED NATIONS PUBLICATION Sales No. E.09.XI.19, https://www.unodc.org/documents /organized-crime/Law-Enforcement/Electronic_surveillance.pdf
[11] Michael Luke Bullock, The Evolution of Surveillance Technology Beyond The panoptic on.
[12] Christian Fuchs, How Can Surveillance Be Defined? Remarks on Theoretical Foundations of Surveillance Studies2010
[13] http://en.wikipedia.org/wiki/Surveillance
[14] Lyon, David. 2007. Surveillance Studies: An Overview. Cambridge: Polity Press.
[15] Sousveillance: Inventing and Using Wearable Computing Devices..., by Steve Mann, Jason Nolan and Barry Wellman, in Surveillance & Society 1(3), 2003
[16] Ressler, Steve, Social Network Analysis as an Approach to Combat Terrorism: Past, Present, and Future Research". Homeland Security Affairs II (2), 2009