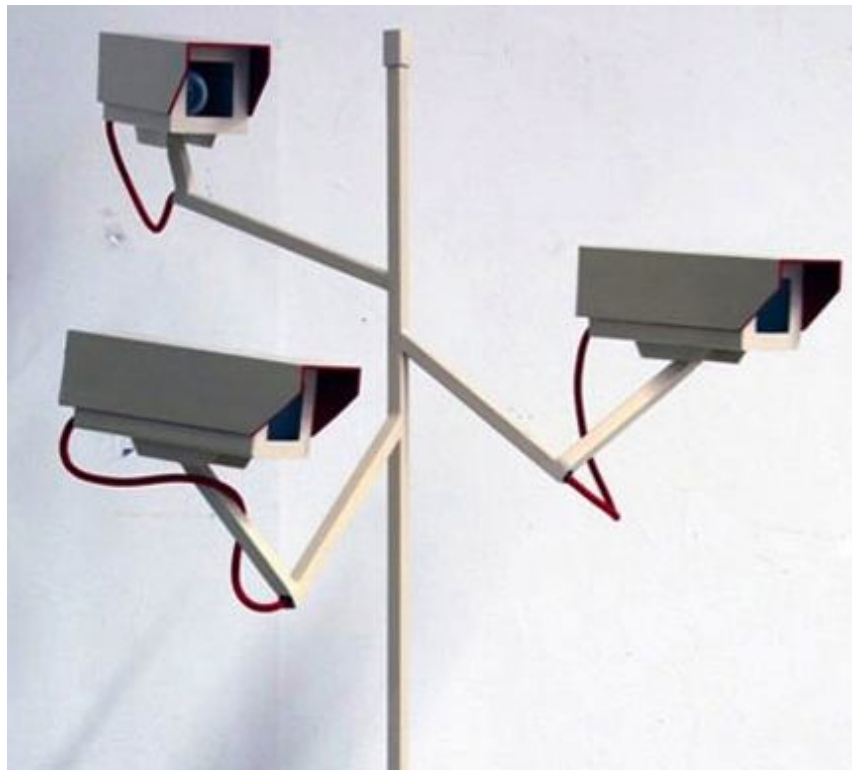


SURVEILLANCE



**Matthew Beckstead
Manny Calderon
Brian Huynh
Terry Moritz**

**MIS 304
Professor Fang, Fang
May 10, 2009**

History

Surveillance has been around for many years. People have used it for many different reasons, but the most common reason seems to be for spying. For example, wiretapping has been around for many years and has been dated back to the American Civil War. When both sides used wiretapping to record messages sent to and back from each side. It was very easy for wiretapping to be utilized back then because messages were sent through telegraph lines. However, when the invention of the telephone came into play wiretapping took a back seat because there was no known way to wiretap a telephone line at that time, as the rate of information passing through the telephone line would flow too rapidly.

Quickly after, the desire for a telephone recording device came to play and the motivation for Thomas Edison's phonograph. However, Edison found that the device was not sensitive enough to do any recording; therefore, he developed the Telegraphone in the late 1877. This was a magnetic recorder specifically designed to record from a telephone line. Then a few years later the American Telegraphone Company fails without producing many of the machines. About the years of World War 1, the Dictaphone Corporation introduced a new phonograph based recorder. This new machine was the most reliable recording device at that time which can record from telephone lines. At this time of period these devices were rarely used as a surveillance tool. They were mostly used by power companies and railroad companies for their own private operation. It was not until the end of World War 2 the technology was used for surveillance purposes.

The invention of the dictagraph was a new step in the progress of surveillance; it wasn't made by the Dictaphone Corporation but it was utilized by private detectives. The major shift came in 1945 with the use of wire and tape recorders becoming readily available. These could easily be modified for personnel surveillance use by consumers. This sparked up the first debates in the court system about whether or not these recordings could be admitted as evidence in court cases. However, these recording devices were bulky and heavy. This limited their portability and usefulness. Surveillance recordings became increasingly common in the 1950's with the invention of the transistor recorder.

After the bringing of the "Pocket" size recording devices, this is when companies started marketing these products to the public. The Minifon, a West German product, was the most popular of these products. The production of these products grew almost parallel with the increase of paranoia of the Cold War. The most popular case of using audio recorders comes from the Oval Office of the President of the United States. With the use of audio recorders, the infamous scandal of Watergate was brought to the public's attention. In today's modern world of Internet and video surveillance, audio surveillance has become very minor. However it can still be very useful. Just like audio recorders video recorders have also been utilized for surveillance purposes.

When people think of video surveillance they mostly think of the camera watching them at the teller window of the bank or maybe the camera watching you as you shop. However, surveillance goes as far back as 1965 with the use of the closed circuit television. In 1965

there are cases of police using closed circuit television to help them fight crime. Closed circuit television cameras were installed in the New York Police department in 1969. Although CCT was useful, video surveillance really took off with the introduction of the video cassette recorders using analog technology. During the 70's the use of video surveillance exploded with the uses being for law enforcement, traffic control, and divorce proceedings. Also companies that were targets for theft began using these systems.

Another industry that utilized the video surveillance practice was the insurance industry. One of the draw backs of the analog technology that was being utilized was its use at night or in low lighted areas. The solution to this was the Charged Coupled Device camera, which used microchip computer technology. Then in the 1990's digital multiplexing technology entered the video surveillance industry. This allowed people to record on several different cameras at one time. This also allowed motion recording and time lapse, which helped cut down on wasted taping. After the drop in price for digital video surveillance, it made perfect sense for companies to utilize this technology as it could potentially save them money in the long run. This gave anyone using video surveillance the advantage of a very clear picture and the ability to improve the picture if so needed. This lead to a second huge increase in the video surveillance practices.

In 1997 police stations across the nation installed digital in their areas. After the 9/11 attacks in New York, software companies began working on technology that would help video cameras recognize people. This is called video recognition technology. In 2002 the

recognition software was installed into cameras at the Statue of Liberty and Ellis Island. Then in 2003 a middle school in phoenix installed the facial recognition software at their school. Although the idea has been met with mixed reviews by faculty and parents, it has been useful in recognizing sex offenders, suspected child abductors, and missing children. It is very clear to see how advancing technology has help video surveillance advance in the last 50 to 60 years.

The most useful tool in surveillance today might have to be considered the Internet. The Internet is not considered a surveillance tool by itself, but it is widely utilized in every aspect of surveillance. With audio surveillance, the internet allows you to listen from almost anywhere in the world, and it also enables you to clean up fuzzy sounds. Also the Internet can let you watch video surveillance from around the world. To be able to do this the use of live streaming video can be utilized. So as you can see the evolution of surveillance technology has been very drastic. Any kind of surveillance systems require that they have the hardware, software, data, procedures, and people to operate. Further along in the paper we discuss parts of these systems and what they are along with today's examples.

Hardware

The first of five component framework includes a computer side which is a combination of software and hardware. Without these two key segments of the framework the other areas wouldn't be possible. Hardware is important in surveillance as it allows monitoring of

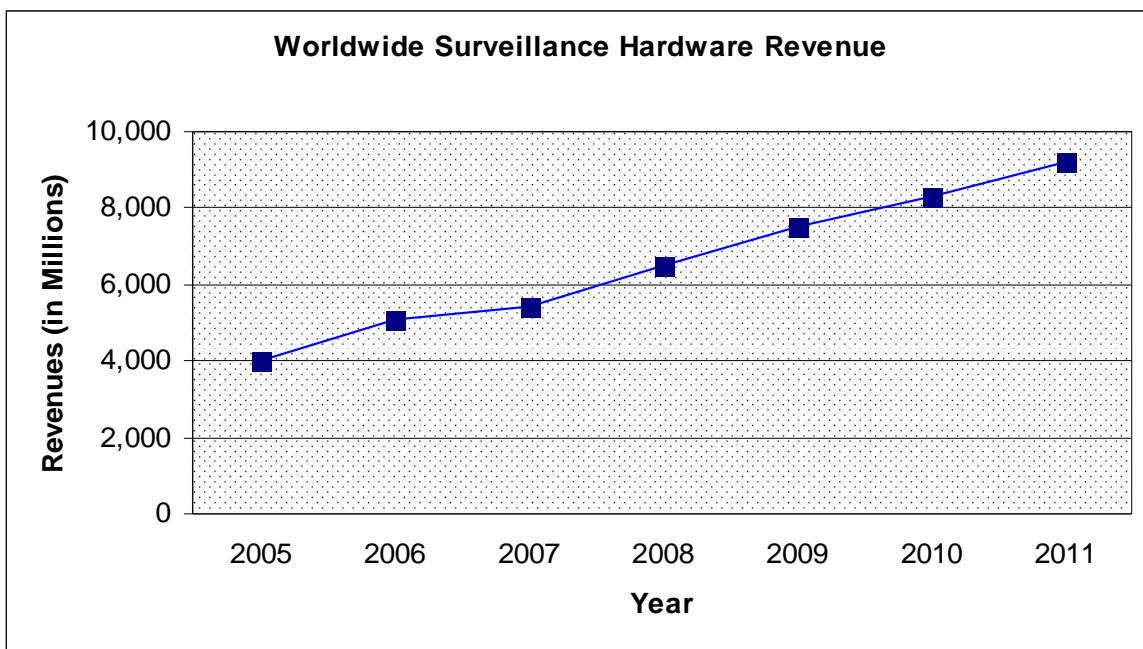
employees via a computer, mobile phone or a camera. Surveillance hardware involves a variety of intricate components to track employees, the premises and technology. Cameras are a critical piece in tracking efficiency and productivity within the workplace or premises. Hardware allows the capability of tracking consumer behavior, records credit and purchasing history and biometrics. Over 200 companies produce biometrics in the United States and gross sales reached approximately 1.9 billion in 2008. The industry is about \$40 billion worldwide and is expected to continue growing at an average of 20% a year.

Some business recommended products include the Cisco PV c2300 which can be monitored via an internet connection. Real-time surveillance is accessible 24 hours a day, including access through a cell phone service. An additional key component of a business camera is the ability for remote control movement. Cisco offers a server network which allows the customer to access a specific date recording via a secure network. The benefit of having a secure outsourced video database disables the ability for employees to tamper with day to day processes.

Phones and vehicles have also been on the rise with surveillance. Small businesses can now integrate systems in company vehicles and mobile phones to track the location of an employee. These hardware and software products increase efficiency and productivity for a company especially due to the 24 hour surveillance capability via the internet. GPS products from \$150 can be purchased and easily installed to enable this service. GPS

tracking helps ensure the employees are at the location needed at a specified time, thus saving the company money and increasing revenues.

Surveillance hardware comes in many forms and devices to meet the individuals or business needs. Many companies specialize in home, business and vehicle hardware surveillance and services. ADT, Brink's and APX are among the largest and most recognized surveillance companies in the United States. These companies track and monitor: fire, carbon monoxide, flood detection, low temperature, gas, video and theft. In most cases they will charge a set up basis price for installation and a monthly service charge. The "Q-SEE" is an effective product offered by some of the companies mentioned, the device allows for the user to play live footage, record, playback and can be accessed through the internet. Features such as night vision, color camera, memory storage and motion sensors are also available on the "Defender" offered by Brink's.



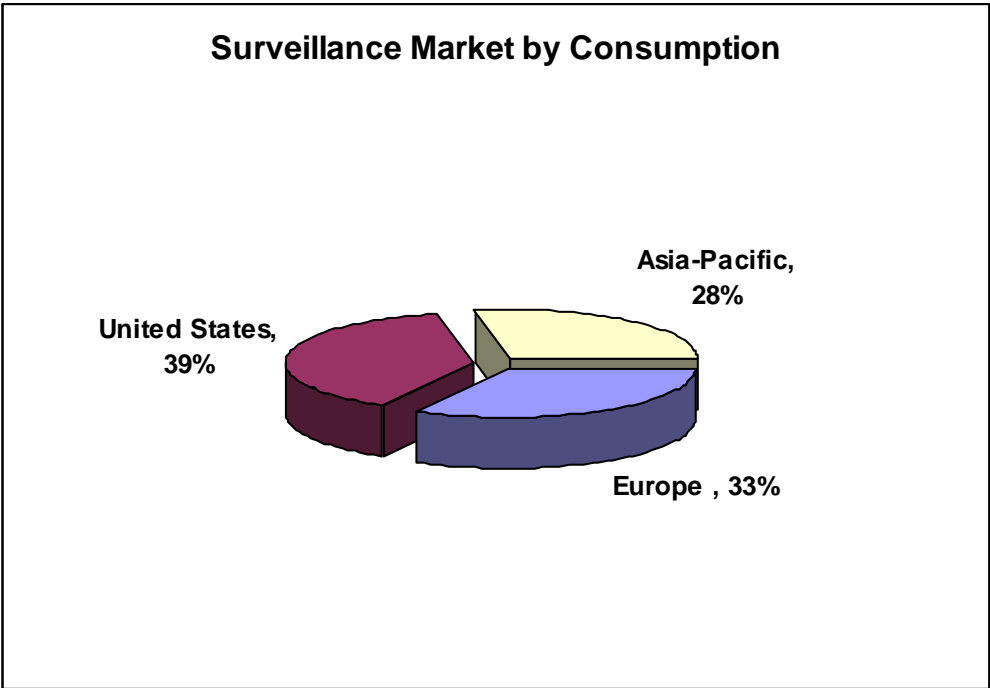
Software

As technology improves, new software needs to be implemented to track new sophisticated technology. Internet surveillance has become a growing field for software producers. Employers want to monitor their employees to assess if an employee is being "efficient" or inefficient. Since the internet has become a powerful tool, most employers cannot completely block access to it but they have added internet limitations to enable only specific websites. Spyware is one of many softwares that can be purchased in the public and enables the tracking of a user's activities and reports it to the administrator; the administrator then reports the information to the employer through various techniques. Additional software like "KEYKatcher" and "Spysure" are also available to track computer progress and activity. Mobile activity and production can be tracked with simple software like "FlexiSpy" and "Mobile-Spy" which are priced as low as \$50 USD.

Additional software is also available to monitor the desktop of a user. This type of programming can usually be tracked and viewed remotely. Other types of software include email tracking to and from employees. Emailing capability in many small business environments ends up being a type of chatting program between employees, thus reducing productivity. Using surveillance software cuts costs by 50% every year. Instead of having someone sit in a room monitoring activity on a business premises a digital signal is now being transmitted via the internet and accessible from anywhere in the world. Surveillance software is also affordable and can be found in many local stores with different options available for a specific need. The most simple surveillance software will help reduce

shrinkage by: deterring potential thieves, monitor cash registers, record evidence to prevent fake accident claims, monitor hazardous work areas and meet insurance requirements.

Since surveillance has improved so much over the last decade, new services have been created to help business improve efficiency and reduce costs. Some available options for businesses are to outsource their surveillance monitoring. A growing market for digital surveillance is growing in countries like India, China and Malaysia. Combinations of hardware and software have given this market strength to grow worldwide. Companies in these countries provide services to monitor employees, intruders, smoke and alert the employer when something looks suspicious. The industry expects to grow at an annual rate of 15% with most of the business coming from North America. This is also an estimate that is difficult to grasp because this is yet another industry that will American jobs abroad.



There are certain limitations on the information that surveillance software can monitor.

Invasion of Privacy in the workplace and in public has always been a very big issue.

Business surveillance also has its limitations implemented by the government. In the United States internet privacy, financial privacy and medical privacy has been a growing issue. Employers are becoming less able to view delicate personal information from employees. Financial privacy includes anything from outstanding debts, purchases and even stocks. Medical privacy is more sensitive than any of the three because it reveals details about one's sexual activity. Data privacy in many instances is not highly legislated or regulated in the United States. Private data is usually accessible by employers when a person is applying for a job. All of these issues are forms of privacy invasion and procedures put into operation by the government.

Surveillance can also be an obstacle for small business because people don't like to be monitored or have their privacy invaded. Most employers today still use the traditional methods of surveillance in order to avoid conflict in the workplace. Typical types of surveillance used in small business are eavesdropping on phone calls, recordings and video monitoring. Through surveillance the employer and employee both benefit by protecting the company. Theft can in many instances become a serious issue and through video surveillance theft can be reduced. One of the core issues with surveillance is privacy, stress and a lack of motivation. Some privacy issues and complaints have been dealt by not informing employees that they are being monitored. In some cases micro-cameras are added to reduce the capability of noticing such device.

Data

The five component framework consists of two sides with a bridge in the middle to bring them together. There is the computer side and the human side which consists of the hardware and software on one side and the procedures and people on the other. The bridge in the middle comes from the data which is collected from the computer side and is to be used by the human side. Data can consist of many different things. For example, it can be a image from a camera, any sound picked up from a microphone, information entered into the computer, and any other information you can think of to put through an information system. The data that is used in the surveillance industry can be identified fairly easy. I will give some examples of the kinds of data collected and interpreted in several different kinds of surveillance systems. The several different types of surveillance systems are as follows, video and camera, E- surveillance (Internet), GPS_and satellite, and home surveillance.

The most common and recognized surveillance is video cameras. These cameras can collect several different types of data. The most obvious data collected is the pictures that are taken from the camera. Also the video could collect sound if it has an audio portion attached. The data that is collected is not very helpful by itself, but when the data gets interpreted it can be very helpful for whatever the purpose is. This data would bring together the human side and the computer side of the five component framework.

A key in the world of internet technology is E- surveillance. The data collected from E- surveillance depends on what exactly the user is looking for. However, data in E- surveillance can range from pictures, text, videos, sounds, and so on. The most useful data for E- surveillance is the data which informs the users of the computers use. It can collect every key stroke, save all downloaded material, save and store emails, and save recent Internet searches. Any information collected from the following areas would be considered data. Another surveillance system is one that uses GPS and satellite technology. This kind of technology is used mostly for tracking location of people or vehicles. The data collected from this surveillance system would be very simple. The data collected would be the signal sent from the tracking device to the satellite and back to the user of the surveillance system. Data provided would be a signal informing the user of the employee's location and vehicle status.

Home surveillance is also another important area of security, this area can consists of a combination of different surveillance systems, or just a very simple home surveillance system which consists of just one technology. With home surveillance the data can be all kinds of different items. Some of the data would be the signal telling the home surveillance system if the house is secure or not. Also, data could be any pictures or sounds recorded by the home surveillance system sent. If the home surveillance system is sophisticated enough then the data that is collected can be a wider range of things.

Surveillance systems that specialize in home security can collect data similar to the satellite technology and the Internet. It can record video, sound, and pictures and send them to the user via the Internet or directly to a mobile phone through satellite technology. As you can see data is a very important part of the five component framework. It might not be the most important, but it is very useful. Without data in the framework then there would be no connection between the computer side and the human side. Therefore, data is the bridge that is very necessary in the five component framework.

People

When it comes to surveillance there are many different people and procedures that are involved. Typically there is a security guard or team in place who physically patrols a given area. These guards are usually supported by some of the various hardware and software much like the ones previously discussed. People are considered to be the most important area in the component framework as people are the users of framework as a whole.

Procedures are important because without proper use the framework will not work or make any sense.

Banks, like many retail companies, usually have their own internal surveillance team in place to support any security guards. This team is responsible for providing the procedures that all the employees for that company will follow. They are in charge of fixing or replacing any surveillance software or hardware. Most banks and retail stores use specific opening and closing procedures to keep the business protected after hours. There are also

situational procedures, like those followed during an actual robbery; set in place to protect the bank and the people of the bank during normal business hours.

Prior to a store's normal opening hours there are specific employees responsible for opening and closing the business. This person or persons will arrive earlier than the rest of the employees and is in charge of turning off the alarms and surveying the parameter to make sure that everything is safe, confirming there is nothing out of the ordinary. Once the "coast is clear", they allow the remaining employees into the building. At the end of the day these procedures are repeated, to ensure the proper closing of the business.

The following are specific procedures trained to employees at a bank. These procedures are set in place for a situation such as a robbery. During a robbery the first thing taught is to stay calm. A bad situation can only get worse if a person panic. The next thing employees are trained to do is to follow the exact instructions the suspect is asking. Do not try to be a hero. Once the robbery is over and the suspect has left the premises the employee is instructed to lock him or herself inside the building, activate the alarm and contact the police. Typically the security department of the business and the police will work together to review tapes and interview all customers and employees involved. Sometimes there are networks set in place, that are utilized in the event a business is robbed or placed in danger. These networks help keep surrounding businesses informed about the dangers so they can be prepared for reoccurring events. Typically if one place of

business is robbed that company will alert other businesses in the area via email or direct telephone call.

Surveillance can be used for internal security purposes as well, for instance, preventing employee theft. Internal security personnel will continuously review video of suspected employees. Another technique used in banks is surprise cash audits, typical procedure in environments with heavy cash flow. Either the internal security team or store managers will count designated registers or cash drawers periodically. Usually businesses suffer more losses from their employees than they do customers or robberies. Random cash audits are put in play to decrease an employee's chances of stealing from the company, thus decreasing the overall monetary loss.

Depending on the type of business some companies will opt to hire an external company for surveillance purposes. Usually these people follow their own procedures that are agreed upon by the company who hires them out. These contracted companies provide a 24-hour service that protects the employees, customers and the business at large. Along with the usual surveillance cameras, these security guards will patrol both the inside and outside of the premises. Their responsibilities have also been known to include enforcing parking rules on the premises.

Procedure

Employees are also trained to follow specific procedures as part of their everyday duties. Something seemingly as simple as clocking in and out for shifts and lunch breaks allow the company to monitor the employees; monitoring productivity and the physical whereabouts of every employee. Employees are assigned login ids and passwords used to operate any software and hardware. These login ids and passwords are distributed by the company. Each login id and password are valid for 1 month to 1 year (depending on the business), once expired the employee must reset their information. This protects each individual employee from any fraudulent use of his or her equipment while at work. Not only does this protect the employees' but it protects the business as well. This procedure helps keep non-employees off company computers and it allows for the company to monitor computer and others equipment from being misused.

Another procedure that is common today is the Currency Transaction Report (CTR). This procedure is a federal requirement in the United States. Since cash is harder to track, all institutions are required to report any cash transactions larger than \$10,000.00. It is not uncommon for banks and casinos to do this procedure on a regular basis. Anytime a customer takes or gives out more than \$10,000.00 then that institution is required to complete a report and send it in to the United States government. This procedure is set in place to prevent money laundering typically used by drug related criminals and terrorists. Similar to the CTR, the Suspicious Activity Report (SAR) is utilized by banks, the post office and local garbage collectors. Anytime these professionals witness something or somebody

doing something unusual they are also required to fill out a report and send it in to the United States government.

People, policies and procedures are constantly changing. In order to offset this, employees are required to go through training procedures in order to learn both operational and situational protocols. These trainings are required to be taken several times in an effort to standardize the safety protocols, thus fostering a safe environment for both the employees and customers. These trainings involve reading manuals, completing online courses, taking tests, role-playing and obtaining certifications. Through the completion of those steps mentioned the information system can be used appropriately and effectively.

Conclusion

In conclusion, without the five component framework working together it would be impossible for surveillance systems to operate on a day to day basis. However one important factor of the framework is the people who maintain and engineer these surveillances; people are who set procedures, collect data, engineer, and maintain software and hardware to achieve some purpose. Surveillance is use for multiple purposes from increasing productivity to business or home security. One prime example mention above was the surveillance systems of banks that require the day to day procedure of all employees. From opening to closing, employees of the bank have procedures and protocol they must follow as they are targets for many things that could go wrong. Banks have a highly tech surveillance system and for good reasons such as to protect their employees in

case of a burglary or even to prevent employees from money laundering. In order for the surveillance system such in banks to operate efficiently all five framework components must come into play. The bank must first have the hardware installed. The hardware must be operated by some kind of software. The software must have a data base to store it's data collected. And finally, employees have procedures they must follow to view and collect the important data that is recorded when in need.

Surveillance has many benefits if used in the right form or manner. It can also become a big flaw for the company if used improperly. Today technology, surveillances is not limited to just cameras. Surveillance also includes the monitoring of cell phones, computers, and GPS. With the right equipment and software cell phones can be tapped, computers can be hacked, and information can be stolen. If an individual desires it is not only possible for the person to track or trace a call and find the location of the caller but they can dig up personal information. Information such as social security numbers, addresses, and even passwords to personal accounts. This is possible by monitoring of computer spy software. This is all without the knowledge of the victim. Of course, this is illegal and is not something that people invented surveillances for but with the desire people can intern any idea into something bad.

Identity theft is proof of stolen information either by using software such as Flexispy, Spyware, Spysure and hardware such as the KEYkatcher. These software and hardware can easily be installed. Has a high success rate and is not easily detectable. Therefore it is

recommended that when using an unknown device you should inspect that device and do not access personal information on that device. This includes public ISP such as airports and school because it is possible that someone can view and use your personal information against you.

Future

The future of surveillances has a great potential as technology improves the same goes for surveillance. As surveillance improves and technology betters, the hardware of surveillance will become smaller and more difficult to detect. For instance, spy cameras can be the size of a pinhole. This means cameras can be place anywhere on the body and be un-noticeable to the naked eye. This might cause privacy issues, but it can also save lives and avoid theft, vandalism and even death. Surveillance will only continue to improve in near future and the possibilities are endless.

Surveillance software will also improve by having the capability to effectively recognize faces and retrieve their information through a data base. This software has already been tested in selected airports in the United States seven years ago. ADT one of the largest security service system company currently used in airports agreed to working together with The Visual Electronic Company, Visionic, to improve face recognition software. This was thought to help prevent terrorist threats since the Sep. 11 attack. Issues such as out of date photos and poor lighting could lead to misidentification and flag huge numbers of

innocent people. Issues involving violations of privacy laws are a constantly struggle and worry for the surveillance industry.

Through completed test in Logan Airport in Boston and Oakland International Airport in California a test of the software returned results indicating a high margin of errors in recognizing faces. The facial-recognition software tested was easily misidentifying people by simple changing of characteristics and disguises. Disguises and changing of characteristics such as hair style, facial hair, aging, and weight gain or lost would tripped up the system. The system then was abandon. However, as time passes and technology improves biometric surveillance will be the future. Biometric surveillance is currently funded for research and development by the government and expects to be the next biggest thing.

Biometric surveillance uses cameras or scanners of biological characteristics to identify individuals, but also can identify individuals by matching of fingerprints and iris patterns. Cars for example in the future instead of using a key to unlock doors and start your engine, it would be possible by the touch of your finger. Another kind of system in the future that could happen with the advancement of technology is the iris pattern matching identifier. For instance, clocking into work would be as simple as scanning your iris. Technology of scanning your iris has already been out and is included in some laptop purchases. This enables the user to either type in a password to login, use your fingerprint, or scan your iris

to identify the user. As time progresses, it is a matter of time when the future will be unimaginable.

Another futuristic project for surveillance is by the military. According to recent news the government is creating a hydrogen powered UAV that can supposedly travel for 24 hours with a single charge. This advancement will help the military in day to day combat when necessary. This plane would carry a camera that can be viewed live through a wireless signal. The UAV, also known as Ion Tiger, is different from all the other surveillance remote control aircraft by its long life; reduce noise, low heat signature, and even low emissions. The Ion Tiger is stealthier than any other of its kind. Possibly in the future this device added with face recognition software can have endless potential.

Bibliography

Morton, David. "History of Surveillance Recording." The History of Sound Recording Technology. Mar. 2006. Recording History. 01 May 2009 <<http://www.recordinghistory.org/HTML/surveillance1.php>>.

Roberts, Lucy P. "The history of video surveillance -- from VCR's to eyes in the sky." Video Surveillance Guide. Mar. 2005. 01 May 2009 <<http://www.video-surveillance-guide.com/history-of-video-surveillance.htm>>.

Olsen, Stephanie. "Can face recognition keep airports safe?" CNET News. 1 Nov. 2001. 01 May 2009 <http://news.cnet.com/Can-face-recognition-keep-airports-safe/2100-1023_3-275313.html?tag=mncol>.

Frank, Thomas. "Face recognition next in terror fight." USA Today. May 2007. 01 May 2009 <http://www.usatoday.com/news/washington/2007-05-10-facial-recognition-terrorism_N.htm>.

Company, Cisco. "Multiple-Use Internet Surveillance Camera." Cisco Security. Jan. 2009. 01 May 2009 <<http://www.cisco.com/en/US/products/ps9945/index.html>>.

"Video Surveillance Systems - Buyer's Guide." Yahoo Small Business. Ed. Buyer Zone. July 2008. Buyer Zone. 01 May 2009 <http://smallbusiness.yahoo.com/r-article-a-40952-m-5-sc-49-video_surveillance_systems_buyers_guide-i>.