LAW ENFORCEMENT’S IMPLEMENTATION OF WIRELESS VIDEO TECHNOLOGY IN THE FUTURE

ARTICLE

California Commission on Peace Officer Standards and Training

by

CARL M. MILLER, JR, CAPTAIN PACIFIC GROVE POLICE DEPARTMENT

Command College Class XXXII

Sacramento, California

JUNE 2002
LAW ENFORCEMENT’S IMPLEMENTATION OF WIRELESS VIDEO TECHNOLOGY IN THE FUTURE

The police officer of the near future will be totally connected. They will monitor high crime areas on their patrol car’s computer or palm-size portable monitors from fixed-site cameras that they can control the pan, tilt and zoom functions. They will access the Internet; check booking photos or police records from their vehicles or hand held devices. They will have the capability to record the real time digitized images on computers instead of cumbersome tapes. They will be able to transmit video from their patrol car cameras to dispatchers or supervisors who will know immediately if they need help or if a vehicle pursuit is too dangerous and should be called off. They will have small cameras on their uniforms, which will record their actions or transmit the real time images in the event of an emergency. Unmanned Aerial Vehicles will patrol the skies at a fraction of the cost of current helicopters, beaming down their wireless images and doing a better job of locating suspects or victims and aiding ground officers.

All of these cameras will dissect the night with infrared thermal imaging or light intensifying technology. Facial recognition software will be used to check the identity of people the police contact or could be used to scan a crowd to search for wanted persons. We are at the threshold of this new world of law enforcement connectivity whose impact will be nothing less than the impact of two way radios in police cars first installed in 1933, but the certainty of wireless video technology is not guaranteed.

When examining the issue of wireless video technology two main obstacles emerge that work against implementation. First, the social and political
opposition to government video surveillance; and second, the technological and economic restraint of the current state of this emerging technology. The United States is in the midst of a tremendous cultural and technological change since the tragic events of September 11, 2001 when terrorists used our commercial airliners as weapons of mass destruction against the World Trade Center in New York City and the Pentagon. This epiphany has changed the way many of us view our lives, our sense of security and our tolerance for inconvenience and decreased privacy. There is a newfound sense of urgency and demand that government must do more than it has done before to ensure our safety. Aspects of everyday life in the future are being debated and decided at this point in time.

At the center of many of these discussions is the increased use of video surveillance. Repugnant to many just a few months before the tragedy, now it seems more acceptable, although some still refer to the use of this technology as Orwellian and Big Brother, a reference to the classic fiction novel, Nineteen Eighty-Four, written in 1949 in post-war England. In his novel, George Orwell describes an abusive, tyrannical government in London that subjects their citizens to constant video monitoring in order to control them.

The irony is that George Orwell’s United Kingdom has been using video surveillance cameras extensively since the 1970s, not to repress the population, but to protect and defend its citizens. The cameras were initially installed in London, England to combat the Irish Republican Army (IRA) who had been waging a terrorist war there since the late 1960s. The United Kingdom population has become the most video surveillance watched in the world. In
2000 there were more than 250,000 closed circuit television (CCTV) cameras transmitting images to police throughout the United Kingdom.\textsuperscript{7}

Surprisingly, most United Kingdom citizens are unbothered by such developments and generally are very supportive of their use and expansion.\textsuperscript{8} Research conducted for the UK Home Office in 1992 found that only 6 percent of adults worried about CCTV cameras. A more recent study conducted in 1996 found that 95 percent were in favor of video surveillance and only 7 percent thought it infringed on civil liberties.\textsuperscript{9} Fear of street crimes was given as the most likely reason for support of police CCTV surveillance.\textsuperscript{10} Street crime rates in and around London have fallen on average 50 percent once cameras were installed.\textsuperscript{11} Police have also noticed a halo effect of the cameras by reducing crime rates in the surrounding areas.\textsuperscript{12} Cases such as the murder of two-year-old Jamie Bulger in 1993 by two older Liverpool boys, and the 1984 Harrods Department Store bombing, where video evidence was crucial in securing convictions, have reinforced public support in the United Kingdom.\textsuperscript{13}

A similar study conducted by Gallup Poll in 1978 found that just 10 percent of the American public was comfortable with the prospect of government video surveillance. By 1997, that figure had jumped to 52 percent approval, and an even larger percentage express willingness to accept video monitoring in various retail settings.\textsuperscript{14} It is suspected the percentage would even be higher in a post September 11, 2001 America.

By contrast a 1999 RAND Corporation Law Enforcement Technology Survey (LETS) found in the United States only 41 percent of local police
departments and 67 percent of state police departments use fixed-site video surveillance cameras. Only 3 percent of local departments and 7 percent of state police departments report making widespread use of this technology and none of rural departments reported making widespread use of it.

While the agencies surveyed felt that video surveillance was an important tool, 69 percent of local departments felt cost was the most inhibiting factor to the implementation of this technology. Most of the small rural or urban departments serving populations less than 25,000 reported cost as a main limiting factor in the use of this technology. Only 7 percent of both state and local departments felt training requirements (human risks) as limiting; 4 percent cited effectiveness or reliability of the technology (technology risk), surprisingly only 1-2 percent cited public opinion as a concern. None cited risk or liability (both unanticipated costs) as a block to implementation.

The Current State of Video Surveillance and Wireless Technology

Police in Tacoma, Washington were among the first in the United States to use CCTV surveillance. In 1993, security cameras were mounted in one crime-ridden neighborhood. Monitoring of open-air drug and prostitution markets helped police make 55 arrests in the first three months of the program. In Baltimore, 16 CCTV cameras were installed in a historic 16-square-block area near the city’s redeveloped inner harbor and Orioles Park at Camden Yards in 1996. The program was expanded when a dramatic drop in crime was experienced. New York City has a program for 24-hour remote surveillance in Central Park, subway stations, housing projects and other public places.
during the 2002 Olympic Winter Games in Salt Lake City, Utah over 400 surveillance cameras, many of them wireless, were used to provide the tightest security at any Olympic event to date.23

Most of these CCTV systems are based on either old hard-wired technology or are video recording cameras for later review in the event of an incident. Video cameras mounted in many of the nation's police cars often serve as silent witnesses as horrific events unfold. Imagine the benefit to the officer and the community if dispatchers, supervisors, or other officers could be viewing in real-time many of the tragedies heretofore only caught on tape. How many injuries could be avoided; how many lives could have been saved?

The hard-wired CCTV’s are costly and usually only allow for one monitor at one location. Wireless technology offers a revolution in the way police will be able to use this technology by allowing real-time images to be viewed at multiple locations and even in the field. This technology has already been deployed in Seal Beach, California, who in 2001 converted many of the city’s bank security systems to a special video server that transmits the output of the bank’s security cameras during an alarm.24 Officers in the field or dispatchers can view the real time images by logging into a security web site.25 “This system gives the responding officer better situational awareness,” says Seal Beach Police Sergeant Dean Zanone who implemented the system through a unique partnership with the banks and a technology company who are paying for the entire system.26 Seal Beach is currently looking into converting their patrol vehicle video cameras to wireless transmitters and recorders.
“As criminals become more violent and better armed, real time situational awareness becomes an imperative for law enforcement,” says Sergeant Zanone.27 Wireless Internet technology and smart video systems can offer law enforcement more critical tools in the fight against crime.

The Future of Wireless Video Technology

As stated earlier, the future benefit of wireless video technology will be in the ability for police officers to access real-time video images in order to achieve the ultimate situational awareness.28 First, let’s identify what streaming video is. According to Mr. Frank Maas, of World Wide Video, a research company in Virginia, any moving image is actually a series of still images shown in fast sequential action. A movie will play at approximately 24 frames (a single still image) per second, television in the US is running at 30 frames-per-second (FPS) and streaming video is anywhere between 15 to 24 FPS. Anything less than 15 FPS and the image becomes choppy. The human eye cannot discern any difference in video greater than 22 FPS. Jerky frame-grabbing technology of 3 to 4 FPS that many computer cameras transmit at can allow for lost action and is not suitable for police use.29 The more frames per second are increased, the more the video file size increases, thus taking longer to transmit.

There are however several impediments to the immediate implementation of wireless streaming video technology. Currently, the military and the government agencies have the ability to deliver 24 frames-per-second video to mobile units via wireless technology, but the cost is prohibitively high, says John
Lusardi, of SL Streaming. Hence the wait until this technology is available for law enforcement agencies at a cost-effective price.

According to Mr. Frank Maas, “Bandwidth is the main obstacle and bandwidth is a very finite number.” Making an analogy to a highway, bandwidth refers to the size of the road. The wider the road or the bandwidth means the greater the number of users who can access a certain frequency at the same time. Transmitting video images takes up a lot of bandwidth. An example of how bandwidth works occurs when accessing a computer network when very few people are using it; information is transferred at a much faster rate. Once a lot of other users try to download on the same network at the same time, the speed is dramatically decreased.

Bandwidth becomes more of a problem for the larger law enforcement agency. While a small law enforcement agency may be able to transmit video images to and from a dozen vehicles in the field, a large agency with a hundred vehicles will definitely experience bandwidth problems with current technology.

With speed decreased, images are delayed in transmission. This delay is called Latency. It takes time to convert files, compress them, send them over a wire or a wireless system then reassemble them on the other end. Latency is the sum total of all these delays. In order for the video to be of the greatest benefit it has to be real-time, which is under ¾ of a second latency.

To get around the bandwidth problem, video images are compressed (file size made smaller). Several methods are used like MPEG (Motion Picture Expert Group), which only transmits the part of the image that changes. The more motion, the more files transferred and the more impact on bandwidth.
Breakthroughs are expected soon in the bandwidth dilemma with technology like Wavelet, which will allow for greater compression and less of an impact on bandwidth.\textsuperscript{35}

At the heart of any wireless video transmission is a wireless local access network, or WLAN. These systems are commonplace and the City of Pacific Grove, California, has such a network installed. Pacific Grove’s system is currently used for data transmissions such as reports and crime data, still images such as booking photographs and Internet access. The system broadcasts on a 2.4GHz band, which has several advantages over 900MHz or 5GHz (see table 1.1). All three bands are considered public bands and do not require Federal Communication Commission (FCC) licensing; however, as wireless networks become more popular, there could be increased interference and a reduction of bandwidth. In December 2001 the FCC began state licensing of UHF 700 MHz frequency with a bandwidth of 2.6 GHz as an exclusive public safety wireless band.\textsuperscript{36} It is estimated that this public safety only band will not be fully operational until 2005.\textsuperscript{37} This step, along with new compression methods should help avoid bandwidth problems in future systems.

<table>
<thead>
<tr>
<th>PRO’S</th>
<th>900MHz</th>
<th>2.4GHz</th>
<th>2.6GHz (not public)</th>
<th>5GHz</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Greater range than 2.4GHz (for in-building LANs)</td>
<td>Global market IEEE 802.11</td>
<td>Public safety only IEEE 802.11</td>
<td>Global market IEEE 802.11</td>
</tr>
<tr>
<td></td>
<td>Higher data rates (10+Mbps)</td>
<td>Smaller antenna</td>
<td>Higher data rates (10+Mbps)</td>
<td>Higher data rates (20+Mbps)</td>
</tr>
<tr>
<td>CON’S</td>
<td>Maximum data rate of 1Mbps</td>
<td>Less range than 900MHz (for in-building LANs)</td>
<td>Not currently for use</td>
<td>Much less range than 900MHz or 2.4GHz</td>
</tr>
<tr>
<td></td>
<td>Limited bandwidth</td>
<td>2.4GHz same as microwave and absorbed by water</td>
<td>Less range than 900MHz (for in-building LANs)</td>
<td>Higher cost RF components</td>
</tr>
<tr>
<td></td>
<td>Crowded bandwidth</td>
<td>2.6GHz close to microwave and absorbed by water</td>
<td>2.6GHz close to microwave and absorbed by water</td>
<td>Large antenna</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Required</td>
</tr>
</tbody>
</table>

Table 1.1\textsuperscript{38}
The WLAN’s antennas are relatively small, only 5 feet tall and several inches wide. They can be mounted on poles, which make them almost unnoticeable on buildings. The cost for each antenna site including all required hardware and battery back up is also relatively small at approximately $3,000 each.39

An overlapping system of antennas allow for roaming. Roaming is the ability of a laptop or other portable workstation to communicate continuously while moving freely throughout an area greater than that of a signal hub or access point.40 Roaming is the most important function of a wireless LAN network.

The laptop or workstation accesses the network through a wireless LAN Adapter inserted in the PCMCIA slot of most computers. These cards cost about $400 each and are the only addition required to a computer to allow wireless access to the network.

Video Transmissions and Privacy Rights

What would cause Americans to accept this invasion of their privacy when freedom of unrestricted mobility has been a cornerstone of democracy? Because many people have become so terrified of violent crime and terrorism, many accept the loss of some personal freedom for a feeling of security. On the surface, video surveillance by police departments in public areas seems to be a noninvasive measure implemented for the well-being of the public.41 It is commonplace for the audience of the nightly news to view footage of bank or store hold-ups. Oftentimes this leads to the arrest of a suspect. In April 1994 a
A bank ATM camera filmed a Ryder truck outside Oklahoma City’s federal office building just before the blast that killed 167 people. That clue helped police track down Timothy McVeigh. Cases such as these make it hard to argue that video surveillance cameras should not be used.

The critics notwithstanding, video surveillance devices in public do not seem to violate any constitutional principles. If these devices were set up to gaze into a private dwelling, however, that would be a different story.

The United States Supreme Court has decided in a long line of cases, most notably in *Katz v. United States* 389 U.S. 347, 88 S.Ct. 507 (1967), that there is no expectation of privacy in a public place. The court ruled that the limits of Fourth Amendment protections against an illegal search did not stop at a physical trespass into a constitutionally protected area. However, some protection is suggested in that the court set forth two tests that since 1967 have been the reference point for other decisions. The first test is expectation of privacy and the second is reasonableness of government search. Neither test is explicitly in the 4th Amendment; however, the 4th Amendment does speak of unreasonable searches and seizures. Therefore it would follow that a person in public cannot have a reasonable expectation of privacy from video surveillance cameras.

Recently, the US Supreme Court stunned the law enforcement community in *Kyllo v. the United States*, 190 F.3d 1041(2001). In this case, the court ruled that the police use of an infrared thermal imaging camera directed to the outside of a residence to detect a marijuana growing operation without a warrant was an
invasion of privacy and a violation of the 4th Amendment protection from government intrusions. Justice Scalia delivered the opinion of the five to four split vote. Justice Scalia, a conservative member of the bench, wrote in his opinion:

> It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology.

Legal scholars see this case as an otherwise conservative court worried about the advancing state of technology. Already cameras exist that can see through clothing enabling the users to conduct the functional equivalent of a strip search without the subject’s knowledge. Although useful to see if a person is carrying concealed weapons, they can also reveal a precise image of intimate anatomical details. Devices that can see through building materials are not far off.

System Security

Security concerns are associated with privacy concerns. While many are willing to trust the police not to misuse the system, they are concerned about unauthorized access. In the United Kingdom, B-grade filmmakers have raided footage from public video cameras to make risqué movies, often featuring unsuspecting couples. Wireless transmissions allow for greater opportunity for the system to be compromised. The previous 56-bit security scheme was relatively easy to defeat.

The Seal Beach Wireless system mentioned earlier relies on two levels of encryption. The first level is a 128-bit WEP (wireless encryption protocol)
solution that generates a unique key every forty-five minutes. The second level uses a virtual private network design using IPSEC (Internet protocol security) or triple DES-type (data encryption standard) encryption. These security measures (and others such as spread spectrum and firewalls) are military-proven and should relax public concerns over the CCTV system integrity.

Strategy Recommendation

The purpose of strategic planning is to create positive change that will lead to a desirable future. Because of the continually changing environment, strategic planning enables an organization to successfully navigate through this environment. Prior to any change, the law enforcement leader should follow several steps towards implementation:

• Assess the community, organization and stakeholder’s readiness for change
• Establish steering committees
• Develop a collective vision
• Strategy implementation
• Acquire resources required for implementation
• Generate short-term wins

When examining alternative strategies relating to the implementation of wireless video in law enforcement, the best approach appears to be a gradual introduction of the technology.

In this strategy, the organization gradually introduces wireless video technology, concentrating at first on areas where there will be the least public resistance. Although public involvement is minimal in this approach, the police
leader should take the opportunity to gauge public support and plan for future expansion of the program. The police can concentrate on converting existing video systems to wireless and phasing in wireless video technology. There is a possibility that much of the existing equipment can be retrofitted to allow wireless applications and police department use and access. Examples of existing security networks that can be converted would be school systems, banks and other business security systems that can be accessed during times of crime.

The next phase can be the most controversial inside the organization and involves converting existing patrol vehicle’s video recorders to wireless transmitters. Depending on the method selected, this technology either exists currently (Internet) or is close to development in a cost effective system. This plan will require substantial buy in from the police officers who will resist being monitored. Officers will have to be shown that wireless video transmission is in their best interests by providing them greater officer safety and event documentation. Of course the likelihood of success is increased and resistance should be less if the agency is already using video recorders in their police vehicles.

The third phase of this strategy will be to place fixed cameras in select high crime areas. Only a few locations should be selected initially and these would be preferably located in remote areas with limited views of residences and crowds. Mobile cameras could also be purchased and moved to temporary locations as crime patterns dictate. As the cameras become more accepted, they can be phased into other areas of the city as well. This will also address
one of the biggest obstacles to the smaller agency, cost. By spreading
purchases over time, initial costs will be held down.

Partnerships with businesses such as insurance companies and grant
funding should also be explored to hold down costs. Before any development of
a wireless video network, police leaders will have to assemble stakeholders and
generate support. Because this will be done incrementally, resistance can be
held to a minimum by tackling the least intrusive applications first, thereby
winning support for an ever expanding wireless video system.

Recommendations

In 1999 the International Association of Chiefs of Police (IACP) addressed
the issues of video surveillance in a published document called “Guidelines for
Closed Circuit Television (CCTV) For Public Safety and Community Policing.” These recommendations are for law enforcement agencies and their
counterparts in private sector security that are using video in public places.
These guidelines, with further community and stakeholder input, could alleviate
most concerns. The main points are:

- Restrict the non-court-ordered use of CCTV to public places, to
  enhance public safety & security in a manner consistent with accepted
  rights of privacy.

- CCTV programs must not be based on individual characteristics, or
classifications, including race, gender, sexual orientation, national
origin, or disability.

- The principle objectives of any CCTV program should include:
  enhancing public safety; preventing/deterring crime and public
disorder; reducing and removing the fear of crime; identifying criminal
activity; identifying suspects; gathering evidence; documenting police
actions to safeguard citizen and police officer rights; reducing the cost
and impact of crime to the community; and, improving the allocation and deployment of law enforcement.

- Information obtained from CCTV use should be used exclusively for public safety and law enforcement purposes only.
- Law enforcement agencies should actively seek consultation and input from their community prior to implementing any CCTV program.

Case Study: Oakland Police Department

Society is experiencing, and will continue to experience, unprecedented technological advancements. These advancements will very soon allow for widespread use of wireless video technology by all law enforcement agencies. However, just the existence of technology is no guarantee that everyone will embrace the technology. Consider the case of Oakland Police Department in California. In 1997 Chief of Police Joseph Samuels saw CCTV cameras in high crime areas as an effective crime-fighting tool and proposed their installation.\textsuperscript{53} Chief Fred Sanchez of Pomona Police Department in California was the Deputy Police Chief in Oakland at the time and remembers being surprised by the level of resistance they received.\textsuperscript{54} Chief Sanchez said that they had support from the neighborhood groups, but didn’t include all stakeholders like the ACLU and the City Council in their initial assessment.

The ACLU and other community groups mounted an anti-camera campaign. The ACLU’s main argument was that camera operators could zoom in and read documents that unsuspecting individuals might be holding and claimed that this would be an invasion of privacy.\textsuperscript{55} This eventually led to City Council changing its mind and recommending against the cameras.\textsuperscript{56}
Chief Sanchez states that if he had to do it over again, he would do more research with community stakeholders, recommend a smaller project with before and after statistics, and then work to expand the system by pointing to tangible results.\textsuperscript{57}

Conclusion

The future of wireless video technology in law enforcement seems almost a certainty. In many ways it is a natural extension of that first two-way police radio that was introduced in Bayonne, New Jersey in 1933. Although video surveillance has played a part in policing around the world for decades, wireless technology is poised to have a dramatic effect on the way law enforcement works in the very near future. But to take full advantage of this emerging technology will require more than just the technological know-how and the financial resources. It will require a greater degree of collaboration, partnership, and a higher level of mutual trust between public safety entities and the communities they serve. The phased-in response seems to be the best way to achieve that end.

The implementation of wireless video technology will require a paradigm shift at every level both within and outside the organization. But the implementation of this technology if approached correctly has the potential to bring the community even closer together and more involved in its police department.

The impact of wireless video technology on the law enforcement agency’s leadership could be tremendous as many factions both internal and external to
the organization may have fundamental opposition to its implementation. The successful integration of this emerging technology into law enforcement will truly require a law enforcement leader of the future; one with vision, communication, leadership and organizational skills. In the final analysis if either the community or the organization would feel better if a wireless video network was not in place, then it should not be, despite its clear advantages.

For further information on this topic, please refer to California POST's Command College Class XXXII Journal Project entitled, How will the implementation of wireless video technology impact small law enforcement agencies by 2007?
END NOTES

9 Ibid.
10 Ibid, 53.
11 Ibid.
12 Ibid.
13 Ibid.
15 Schwabe, Challenges and Choices for Crime-Fighting Technology,, 15.
16 Ibid.
17 Ibid., 16.
18 Ibid.
19 Ibid.
21 Ibid., 4.
22 Ibid.
25 Ibid.
26 Dean Zanone, Sergeant, Seal Beach Police Department, interview by author, Seal Beach, CA. (December 17,2001).
27 Ibid.
30 Lusardi, interview.
31 Maas, interview.
32 Ibid.
33 Ibid.
34 Ibid.
35 Ibid.
39 Ibid., 22.
40 Ibid., 13.
41 Angel J. Pompano, “Privacy in the Age of Video Surveillance - This is not Your Fathers Candid Camera,” Yale- New Haven Teachers Institute, 2000, 3.
42 Ibid.
43 Ibid., 5.
45 Pompano, “Privacy in the Age of Video Surveillance...,” 5.
47 Ibid.
49 Ibid., 5.
51 Ibid.
54 Fred Sanchez, Chief, Pomona Police Department, interview by author, Pomona, CA. (January 7, 2002).
55 Ibid.
57 Sanchez, interview


Lusardi, John. CEO, SL Streaming, Inc.. Interview San Diego, CA. (December 8, 2001).

Maas, Frank. CEO, World Wide Video Research Co.. Interview Culpepper VA. (December 14, 2001).


Pompano, Angel J. “Privacy in the Age of Video Surveillance - This is not Your Fathers Candid Camera,” *Yale-New Haven Teachers Institute*: 2000.

Sanchez, Fred. Chief, Pomona Police Department. Interview, Pomona, CA., (January 7, 2002).


Zanone, Dean. Sergeant, Seal Beach Police Department. Interview, Seal Beach, CA. (December 17, 2001).