



Covert Video Surveillance

Includes surveillance training information at end of article



By Jack Ryan, J.D.

Written For and Distributed by Public Agency Training Council. For duplication & redistribution of this article, please contact the Public Agency Training Council by phone (1.800.365.0119), or by email (newsletter@patc.com).

An investigative tool which causes a great deal of discomfort for agency employees is the use of covert surveillance equipment. Investigators should consider the ramifications that may result from the use of covert video cameras before employing them. These ramifications sometimes go far beyond legal ramifications due to societal thoughts that covert video is one of the most invasive techniques of investigation available. The legality of covert video surveillance rests largely in the nature of the area under surveillance. Is the area one where a person would have an expectation of privacy and if so, is that expectation of privacy one that society is willing to accept as reasonable.

A recent case from the Supreme Court of Alaska is instructive as to the analysis when dealing with an employee's right to privacy from covert video surveillance.¹ In *Cowles*, University of Alaska Police officers received information that the University's box office manager was stealing money from ticket sales. The police, without obtaining a search warrant, installed a hidden camera in an effort to catch Lindalee Cowles in the act of stealing money. Prior to installing the camera an audit was done which verified a substantial cash shortage from the box office. The video surveillance lasted for two and a half hours on a Monday morning and was successful at catching Cowles in the act. The court made note of the fact that Cowles' desk, which the camera monitored, could be seen through the ticket window as well as from an open interior door to the office. The court further noted that there was a constant flow of employee traffic around Cowles' desk throughout the surveillance.

In its review of the surveillance the court pointed out that the test used to determine whether a particular technological monitoring is a search is the "expectation of privacy

¹ *Cowles v. Alaska*, 23 P.3d 1168 (Alaska 2001).

©2008 Article published in the free PATC E-Newsletter

Link to Article online: <http://www.patc.com/weeklyarticles/covert-video-surveillance.shtml>
www.patc.com | www.llrmi.com | www.fsti.com | www.school-training.com | 1-800-365-0119

test.” Specifically, did the person have an actual expectation of privacy and is that expectation one that society is willing to accept as reasonable. The court concluded that Cowles did not expect her activities to be monitored therefore she had a (subjective) actual expectation of privacy in her office. The court then focused on the public nature of Cowles’ office in concluding that Cowles’ expectation of privacy was not an expectation that society would be willing to accept as reasonable. The court noted that activities that are open to public observation are generally not protected by the Fourth Amendment. Similarly, “what a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.”

In analyzing whether Cowles’ expectation of privacy was one that society would be willing to accept as reasonable, the court noted the visibility of Cowles’ desk from both the ticket window and interior of the office. The court further noted the constant traffic of employees around Cowles’ desk. The court also pointed out that “when an individual enters into an employment situation with high security requirements, it becomes less reasonable for her to assume that her conduct on the job will be treated as private.” The court found that since Cowles’ job involved the fiduciary responsibility of exchanging tickets for cash, she sat in a high security position with a diminished expectation of privacy.

A case from the Court of Appeals of Ohio is also instructive.² *Brannen v. Board of Education* involved a covert camera placed in an employee break room. A supervisor, suspecting custodians were loafing in the break room for a large portion of their shift, received permission to install the covert camera. The camera was successful in catching the employees taking unauthorized breaks. After accepting discipline the employees filed suit for, among other things, a violation of their Fourth Amendment rights.

In analyzing the case, the court asserted: “An employee’s expectation of privacy in the workplace must be assessed in the context of the employment relation on a case-by-case basis. The operational realities of the workplace may make some employees’ expectation of privacy unreasonable. A public employee’s expectation of privacy in the workplace may be reduced by virtue of the actual office practices, work procedures or regulation. Some government offices may be so open to fellow employees or the public that no expectation of privacy may be reasonable.”³

² *Brannen v. Board of Education*, 761 N.E.2d 84 (Ohio Ct. Appeals 2001).

³ *Brannen*, at 91 (citing *O’Connor v. Ortega*).

In reviewing the circumstances of this case, the court concluded that since other employees had free access to the break room at all times, no employee could claim an expectation of privacy in the area.

The court determined that even if the custodians had been able to establish an expectation of privacy, the search would have been reasonable. The search was justified at its inception since the purpose of the camera was to confirm or deny suspicions that the custodians were taking the extended breaks. The court pointed out: “The mere fact that the observation is accomplished by a video camera rather than the naked eye, and recorded on film rather than in a supervisor’s memory, does not transmogrify a constitutionally innocent act into a constitutionally forbidden one.”

A covert surveillance case from the 9th Circuit Court of Appeals establishes the important distinction between administrative and criminal investigations. In *Taketa*, a DEA agent reported to her supervisor that another agent, Taketa, had shown her how to turn an authorized pen register into an unauthorized wiretap to record conversations. Agent Taketa shared an office at McCarran Airport in Las Vegas with Thomas O’Brien of the Nevada Bureau of Investigation. O’Brien was also involved in the illegal wiretapping. The DEA began an internal investigation and entered the airport office using a key from headquarters. The investigators examined the feasibility of putting in a covert camera the next time the Taketa sought authorization for a pen-register. In its review of this first entry, the court applied the standards announced in *O’Connor v. Ortega* in holding that the first entry was reasonable.

In May, Taketa sought such an authorization and the investigators returned to the airport office. Unable to find the recording equipment, the investigators had to force open O’Brien’s door with a plastic card to gain entry. The investigators found the recording device. They then placed a covert camera in the office. This investigation led to the arrests of Taketa and O’Brien. In its review of the covert surveillance, the court held that the video evidence had to be suppressed. In so holding, the court determined that since O’Brien’s office had been locked, investigators should have obtained a warrant before entering. In addition the court concluded that once the investigation changed from an internal investigation to a criminal investigation, the standards from *O’Connor v. Ortega* no longer applied, rather the more stringent standards of probable cause and a search warrant were required.

SURVEILLANCE TRAINING

<http://www.patc.com/courses/investigation-surveillance.shtml>

Practical Surveillance Techniques in Criminal Investigations

Length of Seminar: 2 Days

Course Overview:

Importance of Having a Case Agent: This session focuses on the absolute need for one or two officers to be designated as case agents who will, regardless of rank, be responsible for the operation. A ranking Officer will always be responsible for the actions of his men and should always receive updates on how the investigation is proceeding. However, the officer working the surveillance operation will have real time knowledge of their target's actions. This knowledge will be obtained by very detailed surveillance reports that will be dissected after every shift and will detail any and activity the officers have with their target.

Predetermined Course of Action if Surveillance is at Risk of Being Compromised: This session focuses on just how far the surveillance is to be pushed, or, just how close officers should come to being compromised. The criteria to be used in this determination should be made prior to the initiation of a surveillance operation, and should be determined by the case agent. Is it best for his case that the target be kept in sight at all times, or, does he want officers to back off rather than risk being "made"? During the inception of an investigation, playing it safe may be the best course of action. Just prior to the execution of a search warrant, losing sight of the target could mean you never see him again.

Counter Surveillance: This session focuses on how far your target is willing to go to ensure his own safety. Counter surveillance equipment and the money needed to purchase this equipment is easily accessible to the criminal element. Your target's equipment will, at times, be superior to your own. Never underestimate the counter surveillance factor.

Prioritizing Your Goals / Understanding Your Target: This session focuses on the need for goals to be set in a surveillance operation. Is a target being followed to determine his residence, to gain names of his associates, or take him into custody? Is the goal to monitor a fixed position, such as a bank, and, if so, have all pertinent factors been taken into consideration? Have possible escape routes been noted? Is a plan in effect if the situation becomes an active shooter scenario? Are the officers conducting the surveillance easily distinguishable from the potential targets? A successful surveillance requires an officer to be acutely aware of and thoroughly understand his surroundings.

Designing Surveillance around Your Target: This session focuses on the case agent's ability to make the surveillance team's job as easy as possible. What does your target like to do on a

daily basis? Does he start the day off at the same breakfast establishment or at the local gym? If he turns right down Steele Street, is that because that's where his girlfriend lives? Historically men are creatures of habit; documenting a few of your target's can be extremely valuable.

Steps in Identifying a Previously Unknown Target: This session focuses on a dozen unobtrusive methods that can be used to identify that new face working the block - Tony Soprano's new driver, or the guy that's been standing across the liquor store for an hour. It also covers the legalities of what the courts have determined to be acceptable actions during car stops and Terry frisks.

G.P.S., Video and Advanced Surveillance Technology / Legality and Court Decisions: The topic of discussion in this portion of the course is technology and its relationship to surveillance operations. Today G.P.S. devices can be placed on target vehicles and provide real time data. Cellular telephones and other small devices capable of being placed on and tracking a target can benefit from the use of G.P.S.. Video cameras, including those purchased on a very limited budget, can transmit wireless images. Thermal and satellite imagery, which are too often overlooked, have become readily available to law enforcement. This session will cover the proper use of such devices as well as the positive and negative issues that can arise. This discussion will also examine case law and court decisions regarding the implementation of such devices and will outline how to determine of court orders become necessary.

Gather Information by Every Means Available: This session will outline several methods of acquiring information that are often over looked - ranging from early morning trash pulls, to several techniques of cross referencing previously obtained data, to Google searches. Surveillance operations can produce tremendous amounts of data and this session reinforces the need to examine even the smallest bits of information.

Surveillance on Foot, Using Undercover Officers and Fixed Positions: This session covers particle tactics for officers following or maintaining visual sight of a target when on foot. It will cover the necessity of pre-planning and the attention to the small details which, if ignored, may compromise a case.

The session will delve into the implementation of an undercover officer and examine their potential to develop a vast array of information from a single conversation with the target or with a close associate. Also covered will be the utilization of the home or business of a concerned citizen for a stationary position and will explore both the benefits it may bring and the inherent dangers of involving citizens in police operations.

Moving Surveillance Techniques, Planning and Choosing Vehicles: In this session we again re-enforce the importance of having a situational plan in place for the surveillance team. Techniques such as the leap frog, running parallel, and consistently changing the lead vehicle all have proven track records. This session will work upon the assumption that your target is a well established gangster, and that he will start looking for you the moment he opens the front door. Participants will learn that in choosing vehicles, team members must take the totality of the surveillance into account. For instance, what is the most popular car in America and just what is

the most popular color? Methods used to make your vehicles fit in to the surrounding environment and keeping them innocuous will be detailed.

Situations That Can Compromise Both Officer Safety and the Integrity of the Operation:

This part of the course will explore many of the unforeseen compromising situations that can arise in any surveillance operation. Real life examples of how improper planning can ruin an investigation will be demonstrated. For instance, how can a simple scenario of two officers sitting inside a van working a bank stakeout easily result in a blown investigation?

If a poorly trained officer is driving down a drug infested street two car lengths behind the target vehicle and, at the stop sign, three dealers run up to his window and trying to make a sale, what is that officer's best move? This session will cover dozens of potential scenarios and provide participants with the guidance and knowledge they need to make good decisions.

Search Warrants, Pre-Raid Surveillance and Trial Preparation: The final session will outline tactics used in developing information for a search warrant, which is very often the goal of surveillance operations. It will cover the importance of having a surveillance team already on location prior to the execution of a search or arrest warrant. It will demonstrate the best and often simplest ways to convey surveillance information to a jury when the case gets to trial, which when done correctly, demonstrates not only an officer's professionalism, but his dedication to the case. Thoroughly cataloged information presented at trial can slam the door on your prisoner's defense strategy in the Courtroom.