



48890 Milmont Dr. Suite 101D, Fremont, CA 94538 | Tel (510) 249-9540 | Fax (510) 249-9545 | www.ojotech.com

The Law and Video Surveillance

This white paper provides an introductory overview of the law regarding video surveillance. It is not a legal opinion. All clients, both public and private, should consult their own attorney if their situation is unusual or they need a definitive answer to a legal question.

First, we identify three uniquely different legal scenarios:

- Government monitoring of public spaces
- Companies monitoring their own semi-public spaces, or areas used by employees
- Private individuals using video cameras

This paper addresses only the first two bullets, above. We provide no information regarding the third scenario.

Government monitoring of public spaces

There are few specific laws either permitting or denying the right of government agencies to install video cameras, or covering the viewing or recording of video from those cameras. Generally, most people's complaints against cameras and recording are based on a perceived "violation of privacy," based on the Fourth Amendment.

As a reminder, the Fourth Amendment to the United States Constitution protects citizens from unreasonable searches. The full text says,

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

There is now a large and consistent set of court cases that provide, for most applications, a clear set of guidelines.

Most court cases ultimately refer back to a 1967 US Supreme Court Decision called KATZ v. UNITED STATES 389 U.S. 347 (1967). In this case Mr. Justice Harlan stated, "The Fourth Amendment protects people, not places."

Justice Harlan in KATZ set forth two requirements that had to be met for the Fourth Amendment to provide protection against government viewing or recording a private act:



48890 Milmont Dr. Suite 101D, Fremont, CA 94538 | Tel (510) 249-9540 | Fax (510) 249-9545 | www.ojotech.com

... first that a person has exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize (objective) as "reasonable."

The general interpretation of these two requirements is as follows.

First, the person must have, "an expectation of privacy." This expectation of privacy includes all spoken conversation. Thus, all audio recording, except in narrow circumstances, is prohibited. At a minimum, the person must be clearly informed that his or her conversation is being monitored or recorded. That notification is assumed to eliminate the inherent privacy expectation of speech.

It is generally regarded that in open public spaces, such as plazas, urban parks and roads, there is little expectation of privacy of actions. A police officer might be observing from a distance, for example. Another member of the public might happen to be taking a still or video picture.

Any remaining expectation of privacy of actions is typically eliminated by the placement of signs indicating that the area is monitored by video cameras.

However, short of extensive signage, the general lack of privacy on public property does extend to all public spaces. For example, a closed phone booth provides a significantly higher expectation of privacy than an open space. A remote and empty area in a wooded park might cause a couple to believe that nobody was watching them. If a camera recorded their actions, they could reasonably argue that they had an expectation of privacy and that their Fourth Amendment rights had been violated.

Bathrooms, changing areas, and locker rooms are never permitted to have cameras. However, these are state laws, not Federal court cases, so details differ across the country. In California, this law is Penal Code §647(k).

The second requirement from KATZ is that society is prepared to accept both the need for cameras and resulting use of the video as "reasonable." This means that the responsible government agency must present a clear and compelling purpose for the cameras. It is best if this purpose is in writing, and has been reviewed and accepted formally by the agency. It is also necessary to have a written procedure to identify which individuals have access to the video, and for what purposes. A log should be kept of all video access.

For example, a property owner was found liable for privacy damages when it was determined that a guard used the cameras in a public lobby to zoom in on women's breasts. Videos that find their way into private movies or get posted on the Internet are likely to fail this second requirement, and thus may make the agency liable for damages under the Fourth Amendment.

Covert cameras may be used for specific and appropriate purposes. For example, a police department may use covert night-vision cameras in a park to catch drug dealers who are violating the park curfew. Police departments should always consult their own legal resources. Typically, a warrant is necessary.

Should a police department or agency find that they have accidentally recorded legal, but private activity, they should note this fact in their log book, then either delete the video or bar officers from seeing it.



48890 Milmont Dr. Suite 101D, Fremont, CA 94538 | Tel (510) 249-9540 | Fax (510) 249-9545 | www.ojotech.com

These responsive actions are important because they identify to the court that the specific, narrow and appropriate purpose of the cameras is being followed. The danger in not following this practice is that the entire surveillance activity could be ruled illegal, and therefore might not be permitted as court evidence.

Companies monitoring their own semi-public spaces or their employee areas

Private companies are held to the same two fundamental requirements as government agencies. One important difference is that there may be a higher expectation of privacy on private property than on public property. For this reason, most private companies usually have signs indicating that an area is under surveillance or video recording.

There are a number of notable exceptions to common signage. 45% of US high schools and a majority of college campuses have cameras. These institutions typically notify their students and staff through regular communications that cameras are installed. They may or may not have visible signs for visitors. However, it is generally felt that there is no expectation of privacy for actions such as vandalism, theft or assault on school property. Also, practical matter, complaints of privacy violations on school grounds are rare. Signage may be appropriate in certain areas, such as around pools or sports facilities.

Many fast-food facilities have outdoor cameras in the drive-through lanes or at the cashier to discourage or prosecute hold-ups. However, the restaurant may not wish to post signs, as the signage might reduce business. Complaints about privacy violations in these locations are unlikely. Employees and contractors should always be notified of the cameras.

Department stores often have low-visibility cameras in order to catch shoplifting and protect against fraudulent accident claims. Again, they may prefer not to post signs so as to not discourage shoppers. Video captures in stores should not be used for any other purpose. For example, if a celebrity were to go into the store, a video of that celebrity should not be seen or distributed to anyone except those approved employees who have a need to look for shoplifting.

Monitoring employee areas requires even stricter adherence to the two requirements. Employees should be clearly informed about which areas are monitored, and why. Changing areas and bathrooms may never have cameras. Cameras may be used to protect a firm against employee theft, and to make sure that major safety rules are followed. Cameras may not be used to prohibit legal activity, such as union organizing, nor may they be used to harass employees. Recordings should never be used for any other purpose, such as making private videos, posting on the Internet, or making fun of employees. Companies should have a written policy regarding videos, and keep a log of all video viewing and usage. Violation of the company's policy could result in damages by the employee against the company.

Audio Recording

Audio recording is almost never a permitted activity under the Fourth Amendment, without a warrant. Recorded telephone conversations must clearly inform all participants at the start of the call or provide a regular beep. Anybody wishing to do audio recording should obtain the written opinion of a qualified attorney.



48890 Milmont Dr. Suite 101D, Fremont, CA 94538 | Tel (510) 249-9540 | Fax (510) 249-9545 | www.ojotech.com

Burglary and monitoring systems that use audio sensors are legal if they are entirely unable to record conversations. This includes burglary monitoring systems and gunshot monitoring systems.

Emergency intercoms may record a conversation initiated by a person in the field. The recording device should play a "beep" once every 12 to 15 seconds.

Looking at private property

Cameras may not look into other people's private property unless there is either a warrant or permission from the property owner. This includes even a fraction of a field of view. For example, a pole-mounted camera in a park might have a corner of the frame that views a portion of a private back yard over a fence. That portion of the frame must be masked off. Most professional surveillance cameras and most software have the ability to implement this masking. Ideally, masking is done in the camera so that video of the private property is never created or transmitted. Doing the masking in software creates the risk that someone might, somehow, get access to the video prior to masking, or perhaps turn off the masking.

Cameras that pan, or move, need to have more sophisticated masking. The mask needs to move in a synchronized fashion with the camera, so that no portion of the private property is ever visible. Fortunately, the best panning surveillance cameras have this feature.

This private property restriction can be a challenge for perimeter monitoring. The property owner installing the cameras should get the written permission of the adjacent property owners, if any of the camera frames might include adjacent property. Most property owners are happy to comply, if your purpose for the cameras is legitimate.

If you do not get this permission in advance, you run two risks. First, suppose you catch a criminal in the act of scaling your fence and stealing. The criminal you catch in the act may ask the court to exclude the video as evidence on the basis that it violates his Fourth Amendment rights. If you do not have your neighbor's permission to film the criminal crossing from his property to yours, the court might possibly agree. Second, there is always the possibility that your neighbor might be very upset when he finds out about the cameras, and could ask for damages on the basis that you violated his privacy.

Sometimes it is possible to place your cameras below height of your fence so that no part of a neighbor's property is visible in the frame. Alternatively, sometimes the camera can be placed at a high angle, so that only your fence and your property are in the frame. Protecting your property from criminal activity also helps protect your neighbor's property.

Even if you have implemented masking on perimeter cameras, you should still discuss this with your neighbors, whether they are homeowners or businesses. Most people do not know about professional surveillance camera frame masking. They might reasonably assume that if there is a camera pointed roughly in their direction, that someone is looking at their property. In a few cases, people have complained that the mere presence of a camera is a violation of their privacy. Talking to your neighbors is both polite, and will likely enhance your overall security.



48890 Milmont Dr. Suite 101D, Fremont, CA 94538 | Tel (510) 249-9540 | Fax (510) 249-9545 | www.ojotech.com

Legitimate Uses

The following purposes of video surveillance systems are common. Under normal conditions, courts will generally consider these purposes to meet the necessary condition of socially acceptable "reasonable" need.

- Theft
- Shoplifting
- Vandalism or tagging
- Gang violence
- Violation of curfew (closed areas after dark)
- Drug dealing
- Safety monitoring in high-risk areas, such as construction sites and docks
- Public safety in airports, transportation, hospitals and high-crowd areas
- Access control
- Replacement or supplement to guards or customer-service personnel
- Safety monitoring around automobiles, boats, and moving machinery
- Monitoring of pharmaceutical handling or cash handling activities
- Monitoring of infants and children
- Monitoring sports events
- Monitoring around police and police facilities
- ATM monitoring
- Casino monitoring of card tables and other gambling areas

Examples

In general, cameras may not monitor public areas without a legitimate purpose.

For example, a camera in a four-space parking garage of an apartment building that had no history of problems might not pass the test of "reasonable" purpose. The tenants might object on the basis that the building owner merely wanted to observe their coming and going. In fact, such activity is not the legal concern of the building owner, and tenants would likely win this dispute.

One of the reasons that courts have upheld the use of "red-light cameras" that record signal numbers is that the cameras take a picture only at the moment that a law is being broken, and they take a picture of only that vehicle. The fact that the cameras "cannot be used for any other purpose" is key to their approval.

Some cities have cameras monitoring traffic at key intersections. The video from these cameras is available to the public over the web. The public benefit of this service is that people can plan their travel. Since anyone can stand on the sidewalk and observe cars, there is minimal expectation of privacy.

However, suppose a third party created software that monitored this traffic web-cam, and created lists of who drove by, and when. Then this third party sold this information. The public could reasonably object



48890 Milmont Dr. Suite 101D, Fremont, CA 94538 | Tel (510) 249-9540 | Fax (510) 249-9545 | www.ojotech.com

that this activity was not a "reasonable" use of the traffic camera. They might demand that the city turn off the camera, or sue to have the third party discontinue their operation.

The use of long zoom lenses has added a new dimension to this argument. Suppose a camera is monitoring a public area for "public safety," meaning people behaving in a way that endanger themselves or those around them. A zoom lens that could read people's cell phones or their luggage tags would be inappropriate. Even if people were aware of cameras in the area, they would not be "expecting" this level of close-up attention. Private information not relevant to the purpose of the cameras could be captured in this instance. Very high zoom-lens cameras have been ruled overly invasive.

Now consider a centrally located pole-mounted camera in a large parking lot. The purpose of the camera is to catch illegal drug dealing in the parking lot. For this purpose it is necessary to capture the drug and money exchange with enough detail to use in court. It is necessary to capture the faces of the participants with enough detail so that identification of the participants is "beyond a reasonable doubt." In this case, a very high zoom lens would be appropriate. In fact, it would be required.

Best Practices

Although the legalities of video surveillance are complex, and we recommend that each client consult with their attorney for legal advice, it is possible to summarize the most common "best practices" in the industry today:

- Post signs warning that the area is under video surveillance
- Select hardware capable of providing a level of detail suitable for prosecution
- Have a written security policy
- Use the recorded video only for the purposes intended
- Keep a log of all video accessed
- Never monitor private areas such as bathrooms or locker rooms
- No audio recording
- Monitoring of any private property other than your own requires permission

Additional Resources

<http://www.yale.edu/ynhti/curriculum/units/2000/3/00.03.05.x.html>