NASSAU COUNTY
SPIN
A Crime Prevention Partnership

SECURITY ADVISORY COUNCIL

THOMAS R. SUOZZI
County Executive

JAMES H. LAWRENCE
Commissioner

DIGITAL VIDEO SURVEILLANCE GUIDELINES

After considering your basic physical security requirements, such as exterior lighting, locks, alarms, and landscaping, a good digital video surveillance system is the next step in protecting your business and providing your employees with a safe work environment. The following are guidelines offered by the SPIN Security Advisory Council to inform the business community of the type and quality of digital video surveillance systems available in today's marketplace. These security recommendations represent an important step towards developing and implementing a sound overall security plan. This document is not meant to take the place of a security professional but was created to provide businesses with general guidelines for maximizing digital video surveillance.

Return on Investment (ROI)

Video surveillance makes good business sense and is a necessary tool in today's vulnerable business environment. Digital video provides not only security but an easy-to-use management tool. Just think of each camera as a dedicated employee, who works 24 hours a day without taking a coffee break, vacation or sick day. Most of all, your electronic employee has a memory that does not forget, is accurate and provides a true return on investment.

The effective use of digital video surveillance equipment can reduce liability & workers' compensation premiums, fraudulent insurance claims, and may assist in the prevention and apprehension of dishonest employees and customers. Today's technology also provides the ability to watch your business remotely from home or other locations.

There are numerous types of cameras and digital video recorders to fit various applications. Entrance/exit cameras, cash register/counter cameras, interior cameras, exterior cameras and digital recorders are the basic components of a digital video surveillance system.

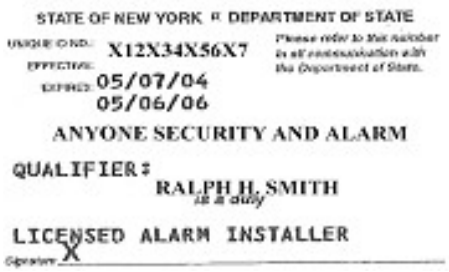
When designing a digital video recording system, it is better to utilize fewer cameras of higher quality recording at higher resolution than utilizing many lower resolution cameras.

How much can I expect to spend?

For a basic four camera digital video recording system for a small retail or office type business you can expect to spend at least $4,500 plus *installation*. Medium, large and enterprise level businesses will spend proportionately more to address their individual security needs.

Installation

It is important that the installer of your system be licensed by the New York State, Department of State, Division of Licensing Services. In addition, you have the right as a consumer to request a certificate of liability insurance from the security vendor.


STATE OF NEW YORK ▫ DEPARTMENT OF STATE

UNIQUE ID NO. X12X34X56X7

EFFECTIVE 05/07/04

EXPIRES 05/06/06

ANYONE SECURITY AND ALARM

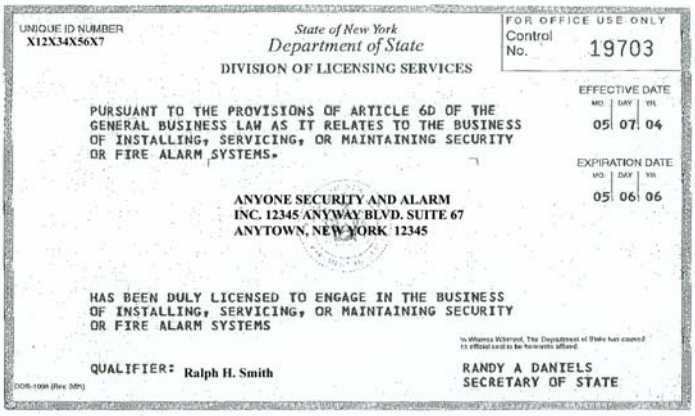
QUALIFIER: RALPH H. SMITH

LICENSED ALARM INSTALLER

(Sample Wallet License)

(To ascertain whether an installer is licensed, go to http://www.dos.state.ny.us/ and click on Search for Licensees and Registrants. CCTV installers are listed under Alarm Installers. Once there, you will have the option of searching by name or business name.)

Licensed installers will possess a wallet identification card containing the name and title of the installer. The Division of Licensing assigns an unique identification number which consists of eleven numbers and is located at the top left hand corner of the license and wallet identification card.


UNIQUE ID NUMBER X12X34X56X7

State of New York
Department of State
DIVISION OF LICENSING SERVICES

FOR OFFICE USE ONLY
Control No. 19703

PURSUANT TO THE PROVISIONS OF ARTICLE 6D OF THE GENERAL BUSINESS LAW AS IT RELATES TO THE BUSINESS OF INSTALLING, SERVICING, OR MAINTAINING SECURITY OR FIRE ALARM SYSTEMS.

EFFECTIVE DATE MO. 05 DAY 07 YR. 04

EXPIRATION DATE MO. 05 DAY 06 YR. 06

ANYONE SECURITY AND ALARM
INC. 12345 ANYWAY BLVD. SUITE 67
ANYTOWN, NEW YORK 12345

HAS BEEN DULY LICENSED TO ENGAGE IN THE BUSINESS OF INSTALLING, SERVICING, OR MAINTAINING SECURITY OR FIRE ALARM SYSTEMS

QUALIFIER: Ralph H. Smith

RANDY A DANIELS
SECRETARY OF STATE

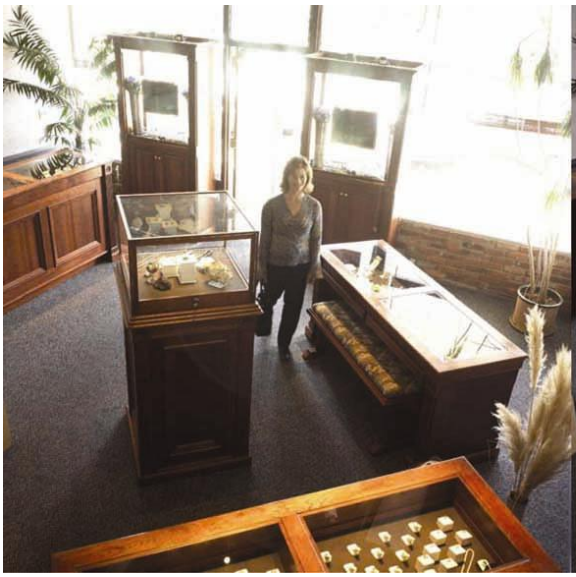
(Sample License)

TYPES OF CAMERAS

- The cameras should be in color with minimum lines of resolution (TVL) of 480 to 540 TVL. **Avoid** 320 to 380 TVL black & white or color cameras.
- If any of your cameras face bright sunlight or look into shadows, they should produce clear video of both situations. See the example below showing how technology can make all the difference. There are enhanced technology cameras available that will produce higher quality video in both circumstances.

- If the camera is utilized in day/night conditions, consider choosing a camera that will automatically switch from color to monochrome (black and white) during low light conditions.
- Each camera lens should be auto-iris and vari-focal which allows for manual adjustment of the field of view and automatic adjustment of light contrast in order to provide the best-detailed video of the people entering or exiting your establishment. **Avoid** cameras with electronic iris lenses.

Standard chip camera



Enhanced technology

TYPES OF APPLICATIONS

Entrance/Exit Cameras:

- Consider placing entrance/exit door cameras on the inside of the building directly along side the doors facing inside the building instead of looking out the door.
- Cameras should be placed as close to 6 to 7-feet above the floor at the door frame, instead of on the ceiling.
- To eliminate tampering, an armored housing with a polycarbonate dome is recommended. This helps eliminate camera tampering, moving direction of camera view, cutting of wires and vandalism.

- Video/photo image should capture the head/face and upper torso of individuals entering or exiting the establishment.

Important Note:

A wide angle view should be avoided here as it renders the image virtually useless for law enforcement identification purposes.

Point of Sale/Transaction Cameras

- Point Of Sale (POS) cameras can be used to record sales transactions and deter employee theft.

Overall View Camera

- May reduce false personal injury and worker's compensation claims, general liability, employee dishonesty, etc.

Restricted Access Area Camera

- May be useful in critical areas such as inventory rooms, money rooms, communication and IT areas.

Additional Considerations

- Depending on the type and location of your business, you may consider installing exterior cameras.

WHY DIGITAL RECORDERS RATHER THAN VCR TAPE RECORDERS?

Videotape Recorders (VCR):

- Old technology that is being phased out
- Low recording resolution and slow recording speed
- Searching for a specific incident is time consuming
- There is limited availability of parts and support
- Requires constant tape changing and maintenance
- No remote viewing capability from home or office
- Costly long-term storage of video tapes

Digital Video Recorders (DVR):

- The resolution and speed of frame capture settings on your digital video recorder is critical in the successful capture of digital video evidence. Without these proper settings, the great looking video you see on your monitor will ***not*** be what is actually recorded.
- Many installation companies tell their clients that they can get 30 days or more out of their digital recorders with four cameras and just a 160-gig hard drive. However, this is only possible if the resolution quality is set to LOW and the record rate is set to SLOW.
- DO NOT LOWER THE RESOLUTION OR SPEED on important cameras (front or main doors, cash register and ATM machines, etc.). Despite the fact that the picture may appear the same on a monitor, it will **not** look the same on playback. Most digital video recorders, when properly configured for high resolution and

speed, will use approximately 5-gigabytes (gigs) or more of hard drive memory space per camera per day for one 24-hour day of digital video. Based on this recommendation you will get approximately eight days of continuously recorded video history and four cameras and a 160-gig hard drive system.

- The recording speed for entrance/exit cameras and cash register/counter cameras should be set at a minimum of 8-Picture Per Second Per Camera (PPS) with a preferred record rate of 12 or more PPS. Other cameras can be set at a lower speed and resolution to save hard drive space for the more important cameras.
- If your unit has motion detection recording capability, make sure each camera is set up with at least 4-seconds of PRE ALARM or PRE EVENT buffer and the same for the POST ALARM or POST EVENT buffer. This is a minimum recommendation; a 10-second buffer is better. This will insure that the recorder will record the incident.
- Setting any digital video recorder at lower than these recommendations may not produce useable quality.
- Digital video recorders should be kept out of sight from employees and patrons.
- Digital video recorders must be kept in a **COOL** and well-ventilated area.
- Test and check your digital video recorder weekly for hard drive operation and video image speed and quality.
- Password protect access to your digital video recorder to eliminate tampering by employees and maintain system integrity.
- In the event of power loss, ensure that your digital video recorder will restart and resume operation without intervention.
- Make sure your digital recorder has the immediate means to OFFLOAD the recorded video without requiring a service call from the installing company. A built-in CD/DVD writer on the unit is easiest; or a unit connected to a PC with a CD/DVD writer can also be utilized.
- Make sure you are trained by your installing company on how to use your system, including off-loading video to a CD/DVD or emailing a video clip.
- It is highly recommended that your digital recorder has an embedded watermark, which prevents video from being tampered with or altered.

Conclusion

These guidelines were developed to assist business owners and managers in navigating the complex world of digital video surveillance. We have taken into consideration the needs of law enforcement, insurance adjusters and the business community to maximize the Return On Investment using digital surveillance systems.

NASSAU COUNTY SPIN

Security Advisory Council

Mission Statement

The Security Advisory Council is a coordinated crime prevention project that seeks to advance public safety and security through public/private partnership and cooperation. Utilizing the expertise of security professionals and police officers, the Council is focused on the establishment of guidelines promoting homeland security, crime prevention and crime reduction techniques, as well as working towards a coordinated response to critical incidents.

SPIN would like to thank the following members of the Security Advisory Council for their contributions in developing these guidelines:

James F. Adelis
President
Adelis International Security

Donald J. Barto
Director of Public Safety
Adelphi University

John A. Bush, III
Vice President
Global Safety & Asset Protection
CA

Mario J. Doyle
Chairman, Long Island Chapter
ASIS International
Regional Director, BuildingStar Corporate Services

Oksana Farber
Law Enforcement Liaison Council
ASIS International
Director of Security, Goldman Associates

Edward Goller
Detective
Nassau County P.D. Electronics Squad

William M. Leahy
Sergeant
Nassau County P.D. SPIN

Marty L. McMillan
President
Intelli-Tec Security Services

James Romagnoli
Director of Security
North Shore/LIJ Health Systems

Matthew J. Simeone, Jr.
Inspector
Nassau County P.D. SPIN

Jerry E. Saltzman
Operations Manager, Crisis Management Center
Citigroup Security and Investigative Services

Douglas Sorenson
Detective
Nassau County P.D. Robbery Squad

David E. Zeldin
Law Enforcement Liaison, Long Island Chapter
ASIS International
President, Investicorp, Inc.

The Nassau County Police Department does not expressly or implicitly warrant, now or in the future, that the use of any or all of the guidelines made in this report shall deter or prevent any criminal activities in and around a premises.

I Spy With My Big Eye:

The Proliferation of Video Surveillance Systems in Northern and Central California

By Mark Schlosberg and Nicole A. Ozer[1]

In 1997 and again in 1999, the Oakland City Council considered creating a video surveillance camera program. The program engendered opposition from the ACLU of Northern California ("ACLU-NC") and several council members voiced strong concerns regarding the privacy implications. Privacy concerns were further fueled by a City Attorney's opinion that records from the surveillance cameras would be available to the public under open records laws. Ultimately the proposal was rejected on both occasions.[2]

While in the 1990s, a number of jurisdictions either rejected camera systems or removed previously existing systems; the national orientation towards privacy and security concerns has radically changed.[3] The events of September 11, 2001 led to a new Homeland Security bureaucracy, flush with money for new security measures. Included in the Homeland Security funding is $800 million for grants to local government for video surveillance cameras and systems.[4]

As the Department of Homeland Security has been handing out money for anti-terrorism purposes, cities and counties throughout the region have been grappling with the very real problem of violent crime in their communities. Residents, facing escalating homicide rates and general concerns about safety have demanded policy solutions from police departments and their elected officials. Security companies have engaged in active marketing to take advantage of community members' concerns and the resources available since September 11. Seeing new opportunities – and using Homeland Security funding in some cases – local government has responded, in part, with surveillance camera systems.

Surveillance systems are often an intuitive solution to residents in high crime areas, their political leaders, and police officials, but so often, little consideration is given to the significant privacy implications of their deployment and use. Even less consideration is given to the long-term results of this significant expansion of the surveillance infrastructure. Camera systems have been approved and instituted in cities throughout Northern California without guidelines to guard against abuse and, in most circumstances, with little or no public debate.

AMERICAN CIVIL LIBERTIES UNION OF NORTHERN CALIFORNIA
111 NORTH MARKET STREET, SUITE 940, SAN JOSE, CA 95113 | T/408.282.8970 | F/408.282.8975 | TTY/415.863.7832 | WWW.ACLUNC.ORG

As the increase in surveillance systems began to be publicly reported, the ACLU-NC started to investigate the extent of video surveillance in the region. We conducted a public records survey of 83 jurisdictions throughout Northern and Central California. While we have not completed the analysis of all the records at this point, even the initial responses point to a significant increase in the use of video surveillance cameras in the region. Over a dozen jurisdictions currently have some type of surveillance program and others are actively considering such programs, further fueling our concerns over video surveillance proliferation and its impact on Californians' privacy rights.

This paper will discuss the ACLU-NC's position on government -funded video surveillance cameras and the current state of video surveillance in Northern and Central California. Part I contains a discussion of the threat posed by public video surveillance to fundamental privacy rights, especially in California; Part II considers law enforcement justifications for video surveillance programs and reviews their effectiveness; Part III reviews our public records survey and its results; Part IV contains policy recommendations and the conclusion.

I. Civil Liberties Implications of Video Surveillance Cameras

> "There was of course, no way of knowing whether you were being watched at any given moment…you had to live, did live, from habit that became instinct, in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized."
>
> -- George Orwell, *1984*

In 1949 when George Orwell wrote the futuristic novel *1984*, he painted a picture of a world without privacy, where government authorities monitored the activities of the citizenry on a constant and continual basis using a wide array of technologies. The loss of privacy shaped society, enabling government control over all aspects of the lives of individuals.

The novel was written at a different time and in a different political context, when the fear of communism and totalitarianism was real and widespread. At the same time, there are strong parallels between the society described by Orwell and the path we are traversing with regard to the government's surveillance capabilities. Rather than communism, the threat is now terrorism and gun violence in high crime areas. While government surveillance is not yet pervasive, we are beginning to move down that path.

In the last five years video surveillance has doubled to become a $9.2 billion industry. J.P. Freeman, a security industry consultant estimates that it will grow to $21 billion in 2010 and predicts that "pretty soon, cameras will be like smoke detectors: They'll be everywhere."[5] Not all of these cameras are government funded and controlled

– there are large numbers of private surveillance cameras as well. Nonetheless, government use of video surveillance is rapidly expanding.

Government surveillance camera programs pose several grave concerns for civil liberties. First, the existence of the cameras themselves carries significant privacy implications. The prospect of 24-hour monitoring of public spaces with video surveillance cameras creates a vast quantity of information on citizens available to the government, allowing the monitoring or tracking of people engaging in wholly innocent and constitutionally protected behavior.

The threat to privacy is amplified by the technological sophistication of new systems. The cameras being installed and considered by cities in California are not the grainy surveillance cameras of yesteryear. Many are state-of-the-art, perched high atop telephone poles with 360-degree views, rolling 24-hours a day. With their DVD-quality video and options for sound, they can zoom in close enough to read and record the book someone is carrying, the name of the doctor's office someone is entering, or the face of the person someone is talking to or kissing goodbye.[6] Everything the camera sees, or potentially hears, can be stored on its hard drive or a central database in perpetuity.

Many of the cameras are also increasingly relying on wireless Internet technology to transmit images from the video cameras to police stations and individual squad cars. Such a system only increases the privacy and security risks. In a wireless system information travels through radio waves in the air. Just like a person could use a police scanner to hear what police are transmitting through radio waves on their in-car radios, a person with a computer and an incentive to hack into the system can intercept the information being transmitted through a wireless system. An individual could use their computer to tap into the wireless network and access the surveillance tapes. The wireless standard was cracked by researchers in 2001 and is widely acknowledged to be very vulnerable to unauthorized access. Recent reports have also shown just how easy it is to pick up the type of 2.4 G wireless surveillance camera footage.[7]

While the use of these sophisticated cameras poses significant civil liberties concerns alone, the implications further multiply when camera technology is combined with new and emerging technologies. It is not far-fetched to think that face recognition technology will soon be used to connect what the camera sees with digital pictures and dossiers about our personal lives. In fact, the Los Angeles Police Department has been testing face recognition software.[8] While the government may not have digital photos of all of us now, this database will exist in the next two years if pressure from the states and from civil liberties groups is not successful in stopping implementation of the federal Real ID Act.[9]

Rushed through Congress in the spring of 2005 as a little-known attachment to an Iraq and tsunami appropriations bill, the Real ID Act requires the creation of a de facto national identity card and national database of personal information by 2008. A state driver's license will not be accepted for boarding a plane, opening a bank account, or

entering a federal facility, unless it complies with the new Department of Homeland Security standards for uniformity. All drivers' licenses will include all of the personal information on the face of the license along with digital pictures in a common machine readable format, all of which will be linked through a shared database available to the 50 states and the federal government.[10]

Similarly, Radio Frequency Identification (RFID) technology could also be easily coupled with the public surveillance cameras. RFID tags, tiny computer chips that can be programmed with any information and then read at a distance by a reader without alerting the holder of the tag, is one of a handful of technologies being considered by Homeland Security as the common machine readable device in drivers' licenses.[11]

The coupling of video surveillance, national identification documents, and facial recognition and RFID technology means that the government will be able confirm the identity of an individual coming into range of a camera and be able to access a wealth of information about that person- likely anything stored in a computerized database- including such things as your motor vehicle and other identification records, your police records and employment history, DNA and drug testing records, and the travel and buying habits of you and your family. [12] The presence of ubiquitous video surveillance cameras will provide a critical structural step toward the creation of a surveillance society. In this context, the use of video surveillance cameras raises three significant concerns regarding the constitutional rights to privacy and anonymity.

First, "Big Brother" surveillance programs threaten to improperly interfere with speech and associational activity. The existence of video cameras in public spaces is tantamount to requiring individuals to register their identity to engage in protest or speak, meet, or walk on the public streets or other public areas. With ubiquitous video surveillance systems, it would be impossible for an individual to be in a public place without worrying that the government was monitoring and recording where they were, who they were, and what they were doing. Such a situation is anathema to First Amendment protections for political activity and protest. [13]

Second, cameras that include audio capabilities may further implicate the Fourth Amendment and California's wiretap statute. While a police officer overhearing an individual's conversation may not be found to implicate reasonable expectations of privacy, the wholesale recording by sophisticated audio systems of the conversations of all individuals passing a camera, smacks of a general warrant in violation of the Fourth Amendment and California wiretap law. General searches that are not confined to an individual, but are a search of every person in a given group are unconstitutional. [14]

Third, widespread use of video surveillance is inconsistent with California's constitutional right to privacy. California voters overwhelmingly approved the privacy right by initiative in 1972 specifically to guard against the expansion of government surveillance and data collection. The ballot argument in favor of the proposition cited "the proliferation of government snooping and data collecting that is threatening to

destroy our traditional freedoms." In *White v. Davis*, the first California Supreme Court to interpret the privacy amendment, the Court noted that

> …the moving force behind the new constitutional provision was a more focused privacy concern, relating to the accelerating encroachment on personal freedom and security caused by increased surveillance and data collection activity in contemporary society. The new provision's primary purpose is to afford individuals some measure of protection against this modern threat to personal privacy. (1975) 13 Cal.3d 757, 774.

Video surveillance cameras coupled with other technological enhancements present just the type of "modern threat" the privacy amendment was focused on.

Moreover, in California public records laws allow access to recordings from surveillance cameras, increasing the privacy threat. Under the California Public Records Act, all government records are open to inspection by the public, subject to exemptions that are to be narrowly construed.[15] Unless video records are related to a criminal investigation, they should be accessible to the general public.[16] In fact the policies of at least one jurisdiction – the City of Fresno – acknowledges that in some cases, video will be accessible to the public.[17]

The implications of public access to video surveillance footage is broad and has not generally been considered by policy makers. Depending on how many cameras are deployed and where they are located, members of the public would be able to request and access video images for a whole host of invasive reasons (*i.e.* an untrusting husband or wife wanting to see if their spouse was entering or exiting a home or business that happened to be in range of a camera, an opposing political candidates wanting to find out who is going into and out of an opponents campaign headquarters, a political organization wanting to identify members of the opposition who happened to have a rally within eye-shot of the cameras.) Widespread video surveillance systems may quickly destroy the ability for individuals to keep their activities private, not just from the government, but also from other private parties.

Finally, in addition to privacy concerns, potential misuse of video surveillance raises significant equal protection issues. Widespread video surveillance systems have also led to discriminatory targeting and other misuse. In Britain, where cameras are already much more pervasive than in the United States – there are over 4 million cameras and in London the average person is captured on camera 300 times a day – there have been documented abuses and targeting of certain groups.[18] Studies published in Britain show discriminatory use of surveillance cameras. Among other issues, researchers found that "the young, the male, and the black were systematically and disproportionately targeted, not because of their involvement in crime or disorder, but for 'no obvious reason.'" The studies also reported that one in ten women were "targeted for entirely 'voyeuristic' reasons by male operators, and that "40% of people were targeted for 'no obvious reason,' mainly 'on the basis of belonging to a particular sub-cultural group.'"[19]

These reports of misuse are not anomalous. In recent years, there have been a number of reported abuses with surveillance cameras ranging from the targeting of demonstrations to the targeting of women and minorities. In 2005, a San Francisco police officer faced disciplinary action for using surveillance cameras at the airport to ogle women. [20] According to Thomas J. Nestell III's recent evaluation of surveillance camera systems in the United States,

> With more than 1 million CCTV surveillance cameras presently in use throughout the United States, standardized controls are necessary. The potential infringement upon persons lawfully protesting, the release of images, and the ability to satisfy voyeuristic desires are real threats to the integrity of CCTV systems and organizations that use those systems.[21]

II. Law Enforcement Justification for Video Surveillance

Not only have the privacy implications of video surveillance systems not been adequately considered, but local governments have also failed to examine the true efficacy of cameras. The primary purported rationale by law enforcement for deployment and expansion of camera systems has been reduction of crime, ranging from violent crime to illegal dumping. Secondarily, officials have also sought to justify camera use as a means of documenting evidence of criminal activity to be used in future prosecution. However, neither of these justifications have been supported by evidence or evaluation.

Crime Reduction

The leading justification provided by law enforcement (and others) for the creation of video surveillance programs is to reduce crime through deterrence. From Oakley where Police Chief Chris Thorsen has claimed that the installation of two cameras in that small community will serve as a "force multiplier" with "deterrent value," to larger cities such as San Francisco where cameras are being installed in high crime areas in response to an escalating homicide rate, cameras are being touted as a crime prevention tool.[22] While it may seem intuitive to policy makers that video surveillance cameras will reduce crime, numerous studies indicate the opposite.

In Britain where camera (CCTV) systems have been in place for close to a decade, criminologists have conducted a number of studies to review their actual impact. One early review was conducted by the Scottish Central Research Unit and evaluated crime statistics preceding and following the institution of surveillance cameras in Glasgow, Scotland. There, researchers found cameras had little impact on crime finding reductions in crime "no more significant than those in control areas without the camera locations."[23]

A broader study in 2002 looked at the cameras' effects on crime in 18 different jurisdictions in Britain. The survey found reductions in vehicle crimes in certain areas –

particularly parking garages– but more significantly, found no impact on violent crime and "in the city centre and public housing setting, there was evidence that CCTV led to a negligible reduction in crime of about two percent in the experimental areas compared with the control areas."[24] These, however, are the very areas where many jurisdictions are deploying cameras.

Finally, the most recent study, conducted by Martin Gill and Angela Spriggs of the University of Leicester, evaluated 13 systems and reached similar results. Despite millions of dollars spent, surveillance camera systems have not had a significant impact on crime. In some areas crime increased, and in some crime levels decreased, but when compared with control areas and taking into account general variations in the crime rate, the changes were insignificant. According to the report:

> All systems aimed to reduce crime, yet this study suggests that CCTV has generally failed to achieve this. Although police-recorded crime has decreased in six out of the 13 systems for which data were available, in only three cases might this decrease be attributable to CCTV and in only two areas was there a significant decrease compared with the control.[25]

Not only did crime fail to decrease as a result of surveillance cameras, but fear of crime also did not decline. In the Glasgow study, researchers found that installing surveillance cameras did not make people less likely to avoid high crime areas.[26] In fact, the recent Gill/Spriggs study demonstrated the opposite – people who were aware of the cameras were actually more worried about crime. The researchers found:

> Respondents who were aware of the cameras actually worried more often about becoming a victim of crime than those who were unaware of them. Knowing that cameras were installed in an area did not necessarily lead to a reinforced feeling of security among respondents.[27]

The failure of cameras to reduce crime (or fear of crime) is also reflected in how offenders view video surveillance. Two studies conducted in 1985 by the Athena Research Corporation surveyed 181 armed robbers in prisons in New Jersey, Texas, Illinois, and an additional 310 armed robbers in twenty state prisons in Maryland, Texas, and Washington. Athena asked about offender planning, methods, and motives and sought to determine what methods were most effective in deterring crime. In both surveys, camera systems and video recording finished in the bottom three in significance behind several other factors including an active police patrol, number of clerks, and number of customers. According to the study, "the robbers say cameras and videos aren't effective and don't keep them from robbing. We know that is true because people rob and kill in front of cameras. One of the reasons they give is that they know that no one is watching at the time, and also they're not worried about being recognized because they can just wear a disguise or get away anyway."[28]

A third offender survey conducted in Britain in 2003 reached similar results. The researchers interviewed 77 convicted male offenders who had committed a prior theft or fraud. Again, offenders did not consider cameras a significant factor and felt that they could avoid detection by wearing a disguise, looking away from the camera, or changing the location or manner in which they committed the crime. The study concluded, "in short, CCTV was not perceived to be a threat by the offenders interviewed. Any potential threat from CCTV was lessened by the speed and manner in which the offense was committed."[29]

Aid in Apprehension and Prosecution

Law enforcement entities also justify cameras by claiming that they will capture evidence of criminal activity and the footage can be used in apprehension or in future criminal prosecution. For example, the London police highly publicized the role of the CCTV cameras in identifying the terrorists suspected of bombing the subway in 2005. Although cameras undoubtedly capture some information that can be of future use, in many ways, the role of cameras has been very limited, often simply providing some assistance to ongoing investigations. While we are unaware of any comprehensive studies showing the extent to which cameras have a positive effect on crime clearance and prosecution, some limited evidence suggests their impact in this regard may not be as significant as expected. Further, the quality of the images collected and the possibility of digital footage being modified or tainted may make it difficult to use as evidence in a prosecution.

First, some evidence suggests that the effect of cameras on law enforcement's ability to clear crimes is not significantly aided by the presence of video surveillance cameras. The Glasgow study cited above, for example, found that "the cameras appeared to have little effect on the clear up rates for crimes and offenses generally. Comparing statistics before and after installation of the cameras, the clear up rate increased slightly from 62% to 64%. Once these figures were adjusted for general trends, however, the research analysts conclude that the clear up rate fell from 64% to 60%."[30]

Second, while some additional crimes will certainly be captured on film, the degree to which cameras assist law enforcement is often greatly overestimated. In Maryland, for example, a spokesperson for the State Attorney's Office told reporters for the *Washington Times*, that the office has not "found them to be a useful tool to prosecutors…they're good for circumstantial evidence, but it definitely isn't evidence we find useful to convict somebody of a crime…We have not used any footage to resolve a violent-crime case."[31]

In Cincinnati, police have also found that cameras are not effective. A University of Cincinnati study found that the city's program, which began in 1998, merely shifted crime beyond the view of the cameras. Police now think resources could be better spent elsewhere. According to Captain Kimberly Frey, "We've never really gotten anything

useful from them…we've never had a successful prosecution…we're trying to use…money for other things."[32]

Finally, police departments hoping to use the camera footage as evidence in prosecutions might find it difficult. The images collected by older cameras are still grainy and make adequate identification difficult. More sophisticated cameras that employ digital imaging may produce clearer pictures, but could bring into question the reliability of the images because the footage could be edited or modified. Camera systems that store digital images in a central database, or transmit images wirelessly to squad cars or police stations, may make the images susceptible to interception and manipulation, both by the government and by outside bad actors.

Monetary Tradeoffs

Spending law enforcement dollars on substantially ineffective video surveillance cameras has repercussions beyond the cost of just the camera systems. The resources spent on video surveillance are not spent in a vacuum. Since public safety dollars, especially in many urban areas, are stretched very thin, the money dedicated to video surveillance is often at the expense of funding other potentially more effective programs such as community policing initiatives and increased foot patrols.[33] Compare the lack of documented success in reducing crime with video surveillance with the remarkable results attained with improved lighting.

A survey commissioned by the Home Office in Britain looked at 13 lighting studies in Britain and the United States and evaluated the cumulative impact. The study found a 20% *average* decrease in crime across the studies with reductions in every area of criminal activity including violent crime. In fact, results were so impressive that in two areas "financial savings from reduced crimes greatly exceeded the financial costs of the improved lighting." The report concluded:

> Street lighting benefits the whole neighborhood rather than particular individual or households. It is not a physical barrier to crime, it has no adverse civil liberties implications and it can increase public safety and effective use of neighborhood streets at night. In short, improved lighting seems to have no negative effects and demonstrated benefits for law-abiding citizens.[34]

These findings suggest that from a law enforcement / public safety perspective alone, the dedication of scarce resources to video surveillance systems may not only be an inefficient and ineffective use of funds, but may also be counterproductive.

III. Public Records Survey and Findings

In light of these concerns and reports of growing use of video surveillance technology, the ACLU-NC conducted a survey of cities throughout Northern and Central California in order to determine the extent of video surveillance systems in the region. In

conducting the survey, we sent public records act requests to 83 jurisdictions throughout the region, selecting a diverse sample (size, location, etc.) as well as the few cities we knew employed video surveillance cameras. We specifically asked about public use of video surveillance cameras, excluding uses in city buildings such as the police department, red light cameras, and police car cameras. We also asked about the types of camera systems that were being considered or had already been deployed.[35] As of this writing, we have received responses from 70 cities, nearly half of which utilize, or are in the process of considering, some form of public video surveillance. While we have not completed the analysis of the documents, a preliminary review points to an increase in the use of video surveillance cameras, with several systems utilizing wireless communication networks.

Ten jurisdictions that we have looked appear to have a program with surveillance cameras being placed on the public streets. Some of these programs are relatively small with just a few cameras being used at this time. Others are broader. Several are currently being expanded. Pittsburg, for example, recently purchased 13 cameras for use at various intersections. San Francisco, whose program started with two cameras in July 2005, now has thirty three cameras, funds set aside in the city budget to install twenty-two more in the coming year, and plans to apply for Department of Homeland Security grant in 2007 for even more cameras. The largest recent expansion occurred in Fresno, CA, where the City Council approved $1.2 million for 256 cameras.

Out of the other jurisdictions that used surveillance cameras, five jurisdictions had a very small number of cameras that focused on one or two particular parks, ten have systems whose scope we are still evaluating, and nine jurisdictions reported that they were considering – but had not yet employed – surveillance cameras.

While the expanded use of cameras alone is disturbing, equally troubling is the fact that several programs are operating without any meaningful regulation. Clovis, for example, which has one of the most comprehensive surveillance systems in the state, has no regulations governing the use of cameras, though the city reportedly is in the process of drafting regulations. Other cities, including Pittsburg and Redding, also lack policies.

Even in jurisdictions that have policies governing camera use, the policies are inadequate and most often, not legally enforceable. In Fresno, for example, the new camera policy, while purporting to prohibit the use of cameras for racial profiling purposes, still allows the use of race as one factor among others, in determining who to monitor. Until community members raised concerns, the policy also specifically allowed the use of cameras to monitor protest activities without any specific criminal suspicion. In San Francisco, the surveillance program grew from two to thirty-three cameras without any binding regulations. Rather, members of the Mayor's Staff and City organizations, such as the Emergency Services Department, promulgated policies that were quickly being modified due to pressure from law enforcement. For example, the camera footage was originally erased after 72 hours (3 days), but was changed to 7 days. It was not until June 2006, almost a full year after the first cameras were installed, that the Board of

Supervisors passed an Ordinance that provides for some legally enforceable regulations about public processes and the use of the cameras. [36]

While the level of surveillance in Northern and Central California is still relatively modest compared with places like Britain or the futuristic world of *1984*, our survey found the use of surveillance cameras to be rapidly increasing and without uniformity or sufficient regulation. At the same time, the availability of additional grant money coupled with fear of crime leads us to believe that these programs – without vigorous opposition and public debate – will expand exponentially over the next several years.

IV. Recommendations and Conclusion

The privacy threats posed by public video surveillance systems are significant and have the potential to radically change the relationship between the citizenry and the government – especially when coupled with other advanced technologies. Despite the privacy implications, local jurisdictions are increasingly moving towards increased use of surveillance cameras with little public debate or consideration of potential consequences. This is a significant mistake.

While the twin goals of reducing crime and apprehending criminals are laudable, the preponderance of the evidence suggests that cameras are at best, only marginally effective in achieving these goals. In light of their limited utility and potential significant negative impact, the ACLU-NC recommends that local agencies stop the deployment of surveillance cameras. Cities should not deploy a technology whose implications have not been fully debated and considered.

Second, any proposed video surveillance program should be subject to intense public scrutiny and debate with a full privacy impact assessment. Local government should also fully evaluate other potential crime reduction measures before considering video surveillance systems.

Finally, jurisdictions that currently have video surveillance systems should conduct a comprehensive re-evaluation of the privacy impact and the effectiveness of their systems. The results of those evaluations should be made public and cities should hold public hearings regarding the future of the surveillance programs and possible alternative crime reduction measures.

While video surveillance may be an appropriate technology to deploy in limited settings, such as in an airport or a police department, it poses a significant threat to privacy rights if used for general monitoring of public space. The programs already in existence and those under development represent a disturbing trend. Even small programs that seem relatively benign have the potential to rapidly expand into larger ones.

Particularly at this time, when numerous agencies at the federal, state, and local level have monitored innocent Californians engaging in First Amendment protected activity, policy makers and individuals should think critically about the deployment of even a single camera. [37] Once money is invested in a program, public agencies become much more willing to spend additional dollars for expansion, rather than critically evaluating programs with an eye towards a new direction. We all want and deserve safe communities, however video surveillance systems are not the answer. Rather than investing money in "Big Brother" programs of marginal effectiveness, governmental agencies should look to policies that show strong empirical results while leaving fundamental privacy rights intact.

---

[1] Mark Schlosberg is Police Practices Policy Director and Nicole A. Ozer is Technology and Civil Liberties Policy Director with the American Civil Liberties Union of Northern California. Research Assistants William Reagon, Fatima Silva, and Lauren Woon assisted with this project.

[2] Brenda Payton, *Cheers for City Council's Rejection of Surveillance Cameras*, OAKLAND TRIBUNE, June 17, 1999.

[3] New York deployed cameras in Times Square for 22 months, but removed them when they led to a paltry 10 arrests, the surveillance cameras in Atlantic City were abandoned when they did not lead to a single arrest, and Detroit dismantled its video surveillance system in 1994 after fourteen years of mixed results and abuse. See ACLU of Northern California Letter to Oakland City Council On Video Surveillance Cameras, May 23, 1997, *available at*: http://www.aclu.org/privacy/spying/14902res19970523.html (last visited October 26, 2006); see also Marcus Nieto, *Public Video Surveillance: Is It An Effective Crime Prevention Tool?*, California Research Bureau, *available at* http://www.library.ca.gov/CRB/97/05/ (last visited October 26, 2006).

[4] Martha T. Moore, *Cities Opening More Video Surveillance Eyes,* USA TODAY, July 18, 2005. The article also mentions an additional $1 billion in money available in state grants.

[5] Moore, *supra*, note 3; Jessica Bennett, *Big Brother's Big Business*, NEWSWEEK, March 15, 2006.

[6] Bulwa, *Future Fuzzy for Government Use of Public Surveillance Cameras*, San Francisco Chronicle, July 23, 2006, *available at* http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2006/07/23/MNGC0K45G21.DTL&hw=surveillance+camera&sn=003&sc=993 (last visited October 24, 2006).

[7] Wireless means that it travels through the air- using the 802.11 specification. 802.11 specifies an over-the-air radio wave interface between a wireless client and a base station

or between two wireless clients. Definition *available at* http://www.webopedia.com/TERM/8/802_11.html (last visited October 20, 2006).

Verton, *Flaws in Wireless Security Detailed: Cracked Algorithm, holes in 802.11 spec mean companies need more authentication,* ComputerWorld, July 16, 2001 *available at* http://www.computerworld.com/securitytopics/security/story/0,10801,62220,00.html (last visited October 20, 2006).

Examples of research detailing 802.11 security vulnerabilities *available at* http://www.cs.umd.edu/~waa/wireless.html (last visited October 20, 2006).

[8] *LAPD experimenting with facial-recognition software.* San Diego Union Tribune, December 26, 2004, a*vailable at* http://www.signonsandiego.com/uniontrib/20041226/news_1n26lapd.html (last visited October 25, 2006).

[9] The National Governor's Association (NGA) estimates that Real ID will cost the states 11 billion dollars to implement. *The Real ID Act National Impact Analysis*, September 2006 *available at* http://www.nga.org/Files/pdf/0609REALID.pdf (last visited October 25, 2006).

[10] See the ACLU Real ID website *at* www.realnightmare.org and EPIC's Real ID page at http://www.epic.org/privacy/id_cards/ for more information about the Real ID Act.

[11] For more information about the use of RFID technology in identification documents, please see *The Use of RFID for Human Identification: Draft Report of the Privacy Committee of the Department of Homeland Security available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_rpt_rfid_draft.pdf ; see also Government Accountability Office Report on RFID technology (May 2005) *available at* http://www.gao.gov/new.items/d05551.pdf http://www.aclunc.org/issues/technology/yes_on_sb_768!_dont_let_your_rights_be_chipped_away.shtml; EFF's RFID page *at* http://www.eff.org/Privacy/RFID/; EPIC's RFID page *at* http://www.epic.org/privacy/rfid/ (last visited October 26, 2006).

[12] Publicly-available databases accessed by the government, such as Choicepoint, collect and sell data on individuals that include the following categories: claims history data, motor vehicle records, police records, credit information and modeling services...employment background screenings and drug testing administration services, public record searches, vital record services, credential verification, due diligence information, Uniform Commercial Code searches and filings, DNA identification services, authentication services and people and shareholder locator information searches...print fulfillment, teleservices, database and campaign management services..." See EPIC Choicepoint page *available at* http://www.epic.org/privacy/choicepoint/ for more information.

[13] *Watchtower Bible and Tract Society of New York, Inc. v. Village of Stratton* 536 U.S. 150 (2002) (ordinance that required individuals to obtain a permit prior to engaging in door-to-door advocacy and to display the permit upon demand violated the First Amendment.); *Washington Initiatives Now v. Rippie*, 213 F.3d 1132 (9th Cir. 2000) (statute that required disclosure of names and addresses of those who were paid to collect signatures for state initiatives unconstitutional).

[14] See *People v. Jackson* 129 Cal.App.4th 129, 163 (2005) citing *Vernonia School Dist. 47J v. Acton*, 515 U.S. 646, 670 (1995) (O'Connor, J., dissenting.) (order authorizing the police to intercept the conversations of "the users" of particular pay telephones is unlawful under California's wiretap statute and violates the Fourth Amendment by failing to particularly describe the persons or things to be seized.").

[15] *See Government Code 6250 et seq.*

[16] *Government Code section 6254(f)* contains an exception for certain law enforcement information.

[17] Fresno's video surveillance policy states that images "shall not be generally releasable to members of the general public," but also indicates that "Images will be held consistent with the Public Records Act" and that exempt materials "include data involving an ongoing law enforcement investigation or data which constitutes an unwarranted invasion of personal privacy." This would seem to imply that many images that do not fall into those two categories would be accessible under the policy.

[18] CBS News, *Close Watch*, April 12, 2002, *available at* http://www.cbsnews.com/stories/2002/04/19/sunday/main506739.shtml (last visited October 25, 2006).

[19] Adrienne Isnard, "Can Surveillance Cameras Be Successful in Preventing Crime and Controlling Anti-Social Behaviors?" *Australian Institute of Criminology*, p. 12 (citing M. Dee, "The USE of CCTV to Police young People in Public Spaces – A Case of Big Brother or Big Friend" 2000, and C. Norris and G. Armstrong, "The Unforgiving Eye: CCTV Surveillance in Public Space," 1998).

[20] http://www.ktvu.com/news/4398749/detail.html (last visited October 26, 2006).

[21] Thomas J. Nestel III, *Using Surveillance Camera Systems to Monitor Public Domains: Can Abuse be Prevented?* Masters Thesis, Naval Postgraduate School, Monterey, CA, March 2006.

[22] Danielle McNamara, *Oakley to Set Up Camera System,* CONTRA COSTA TIMES, July 18, 2006; Demian Bulwa, *Future Fuzzy for Government Use of Public Surveillance*

Cameras, SAN FRANCISCO CHRONICLE, July 23, 2006 (San Francisco Mayor's office claims cameras are deterring crime).

[23] *The Effect of Closed Circuit Television on Recorded Crime Rates and Public Concern about Crime in Glasgow*, Crime and Criminal Justice Research Findings No. 30, The Scottish Office Central Research Unit, 1999 (hereinafter "Glasgow Study").

[24] Brandon C. Welsh and David P. Farrington, *Crime Prevention Effects of Closed Circuit Television: A Systematic Review*, Home Office Research Study 252, August 2002, at p. iv.

[25] Martin Gill and Angela Spriggs, *Assessing the Impact of CCTV*, Home Office Research Study 292, February 2005, at p 58.

[26] Glasgow Study, *supra*, note 22.

[27] Gill and Spriggs, *supra*, note 24.

[28] Rosemary J. Erickson and Arnie Stenseth, *Crimes of Convenience: A Study of What Motivates Robbers Finds that Conventional Wisdom May be Wrong*, 1996, *available at* http://www.security mamagement.com/library/000236.html; Rosemary Erickson, Armed Robbers and Their Crimes, Chapter 4, 1996, *available at* https://www.securitymanagement.com/library/000235.html.

[29] Gill and Loveday, *What Do Offenders Think About CCTV*, 2003, p. 24

[30] Glasgow Study, *supra*, note 22.

[31] Matthew Cella, *Statistics Show Cameras Limited in Decreasing Violent Crime*, WASHINGTON TIMES, August 14, 2006.

[32] Christina Ramirez and Lisa Hoffman, *Video Becomes a Crime Fighting Tool*, CAPITOL HILL BLUE, June 23, 2006.

[33] For information about effectiveness of foot patrols in decreasing crime and fear of crime, *see e.g.* Bethan Jones and Nick Tilley, *The Impact of High Visibility Patrols on Personal Robbery*, HOME OFFICE FINDINGS 201, 2004 (citing 16% reduction in personal robbery in study area compared with 5% increase for the rest of the police force); David Dalgleish and Andy Myhill, *Reassuring the Public: A Review of International Policing Interventions*, HOME OFFICE FINDINGS 241, 2004 (foot patrols decrease fear of crime).

[34] David P. Farrington and Brandon C. Welsh, *Effects of Improved Street Lighting on Crime: A Systematic Review*, HOME OFFICE RESEARCH STUDY 251, August 2002, p. 42.

[35] Other information requested included crime statistics before and after camera deployment and information about funding sources.

[36] San Francisco City Ordinance *available at* http://www.sfgov.org/site/uploadedfiles/bdsupvrs/ordinances06/o0127-06.pdf (last visited October 26, 2006).

[37] See Mark Schlosberg, *A State of Surveillance*, AMERICAN CIVIL LIBERTIES UNION OF NORTHERN CALIFORNIA, July 2006 (discussing surveillance of political activists in Northern California by federal, state, and local agencies since September 11, 2001).