Critical Infrastructure Monitoring System: CIMS

SYSTEM DESIGN AND FUNCTIONALITY OVERVIEW

METRO BOSTON
HOMELAND SECURITY

BOSTON BROOKLINE
CAMBRIDGE CHELSEA
EVERETT QUINCY REVERE
SOMERVILLE WINTHROP

A-1

What is CIMS?

- The Critical Infrastructure Monitoring System is a regional network connecting the 9 communities in the Metro Boston Homeland Security Region. The region includes the communities of:

Cambridge
Boston
Somerville
Revere
Everett
Chelsea
Winthrop
Quincy
Chelsea

What are the major componen of the CIMS system?

- The CIMS system has two components:
  - **A secure network including both fiber and microwave connections linking each of the Metro Boston communities**
  - **Video cameras located in areas of critical infrastructure such as major roadways, chemical, biological or radiological facilities, and other sensitive areas as identified by each community**

Functionality of each compone

- Secure Network: The CIMS project has created a secure network linking each community that uses fiber optics and microwave technology. This network provides each community with an alternative route for data, radio, and video traffic in the event that our traditional communications links are down. This ensures the critical ability to communicate between our communities in the event of a major incident or disaster.

System functionality (continued):

- Video Cameras: Cambridge will receive 8 video cameras to monitor critical infrastructure – specifically major intersections and evacuation routes. The camera locations include:

364 Rindge Avenue
Mount Auburn Hospital
Porter Square
Inman Square
Harvard Square
Memorial Drive @ River Street
Kendall Square
Central Square

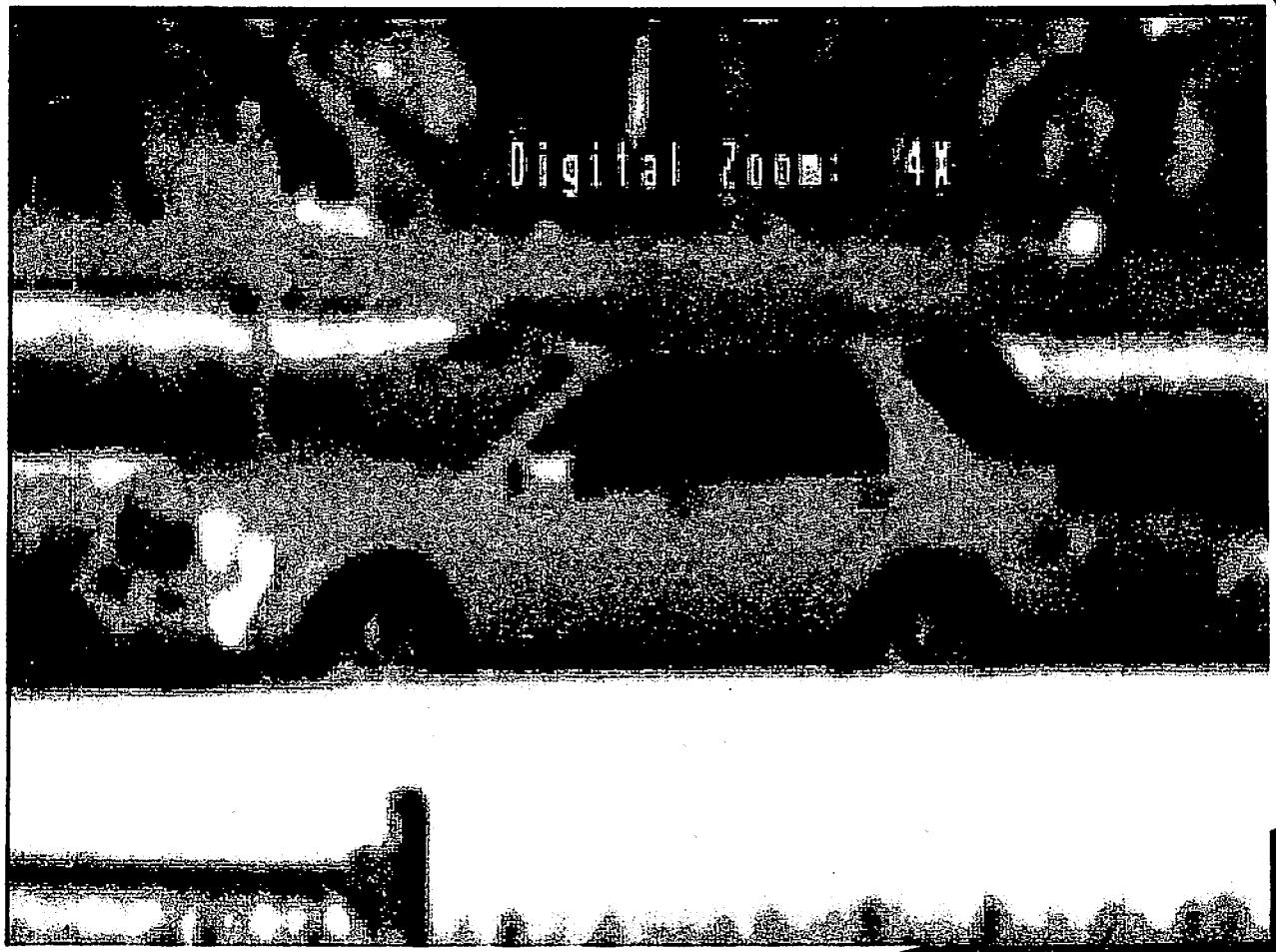
What will the field of view be for the cameras?

- The "home view" for each location will be the intersection or roadway that is most in the view of the camera. Each camera has pan, tilt and zoom capability allowing the camera to be moved and refocused based on need. For example, the Inman Square camera may be moved from a view up Cambridge Street looking east to view up Hampshire Street to determine the cause of a traffic backup.

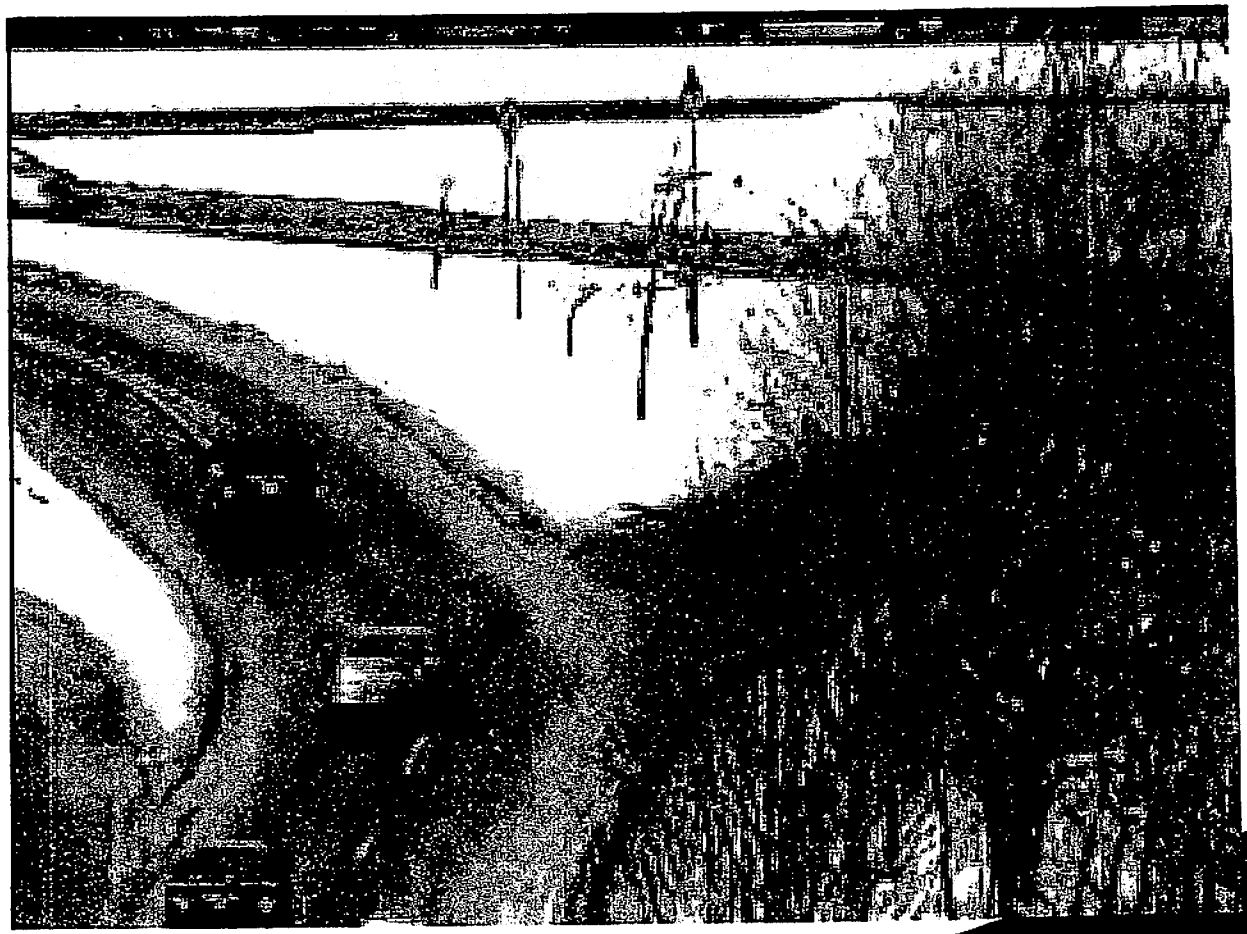
Sample views from some of the cameras:

- The following slides are actual sample views from a few of the cameras. The images include:
  - Digital Zoom: This is a maximum magnification with digital enhancement
  - Analog Zoom: This represents the maximum optical zoom
  - Home View: This is the default view of the camera when not subject to user intervention

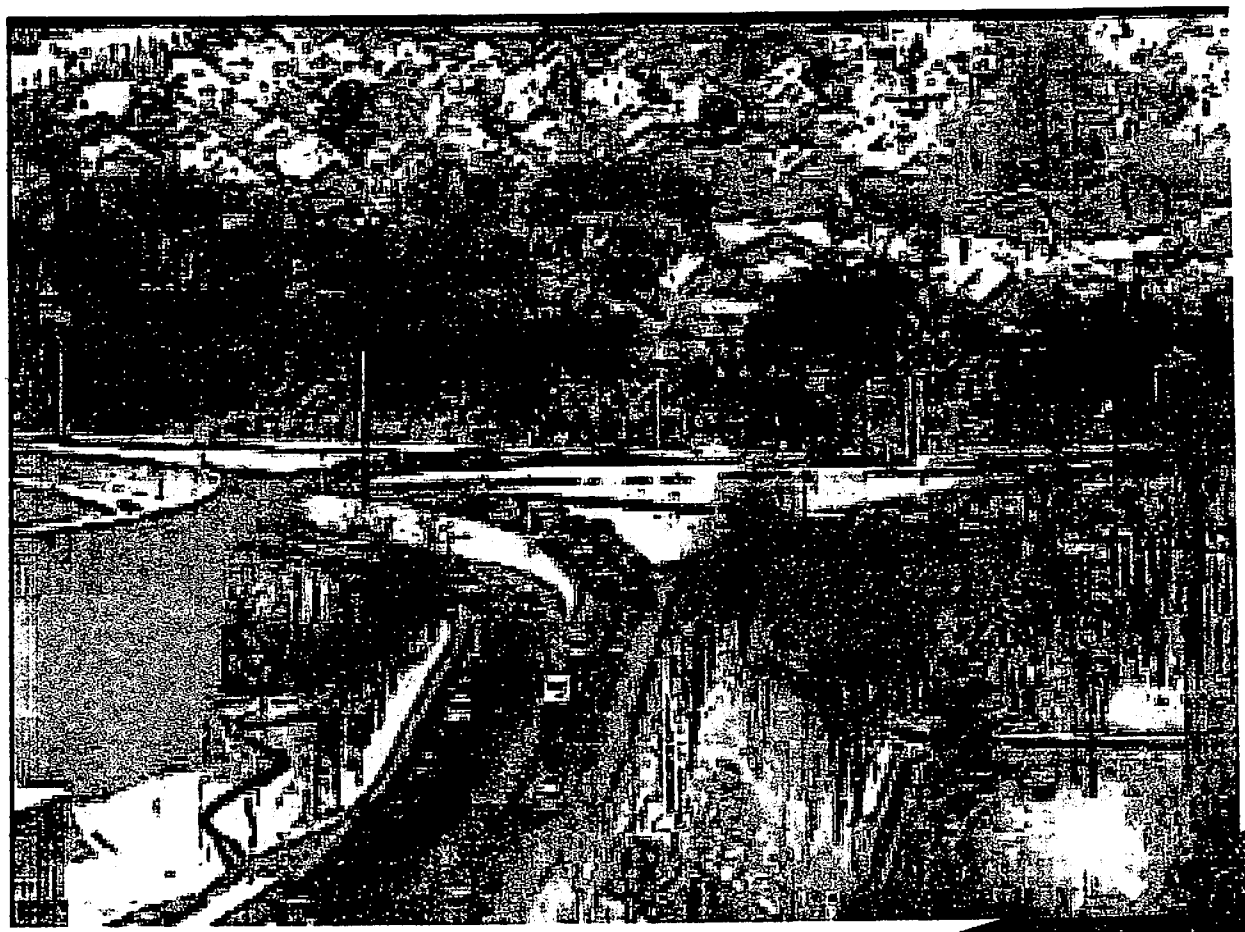
364 RINDGE AVE
"DIGITAL ZOOM"



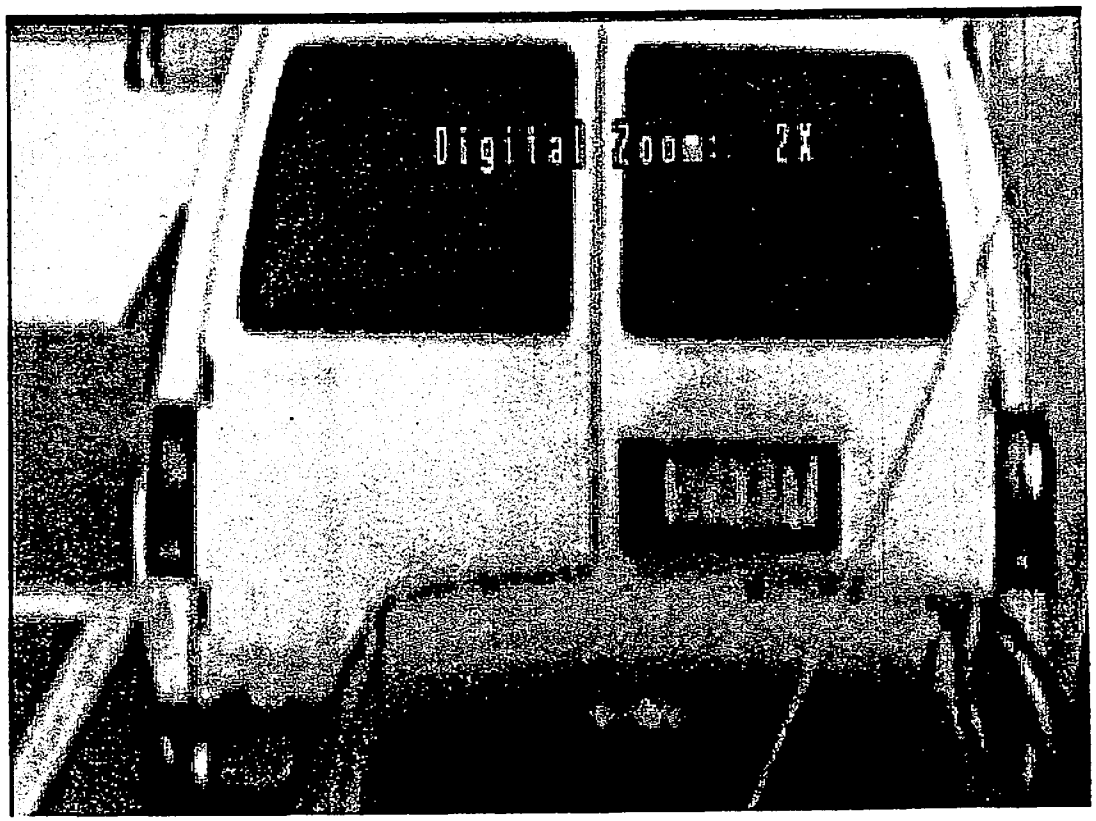
364 Rindge Ave
"Analog Zoom"



364 Rindge Ave
"Home View"

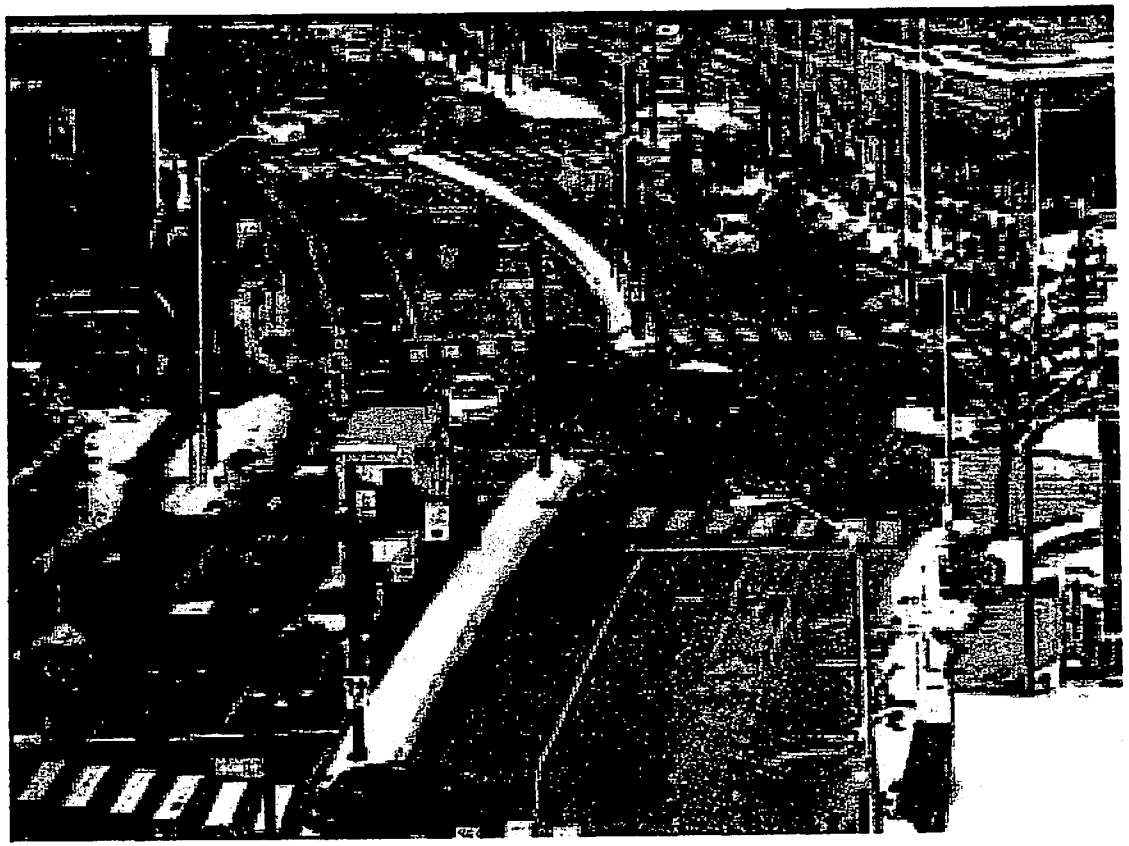


PORTER SQUARE
"DIGITAL ZOOM"

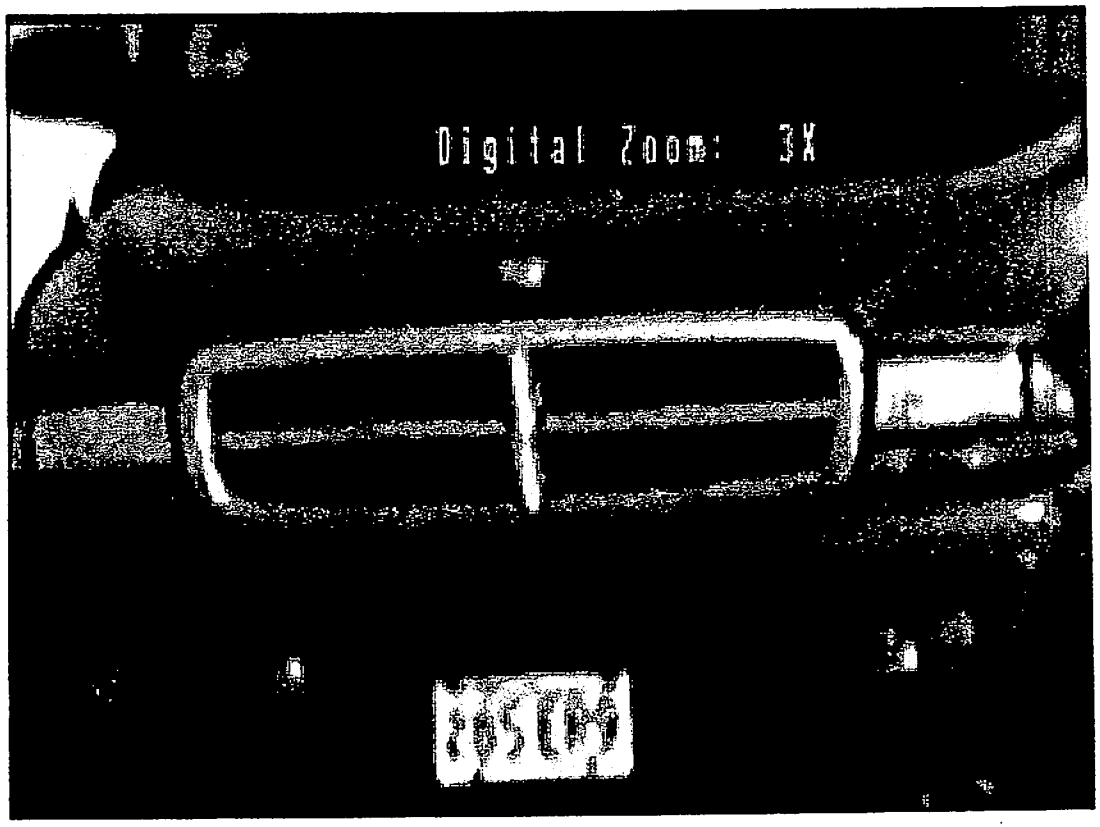


Porter Square
"Analog Zoom"

Porter Square
"Home View"

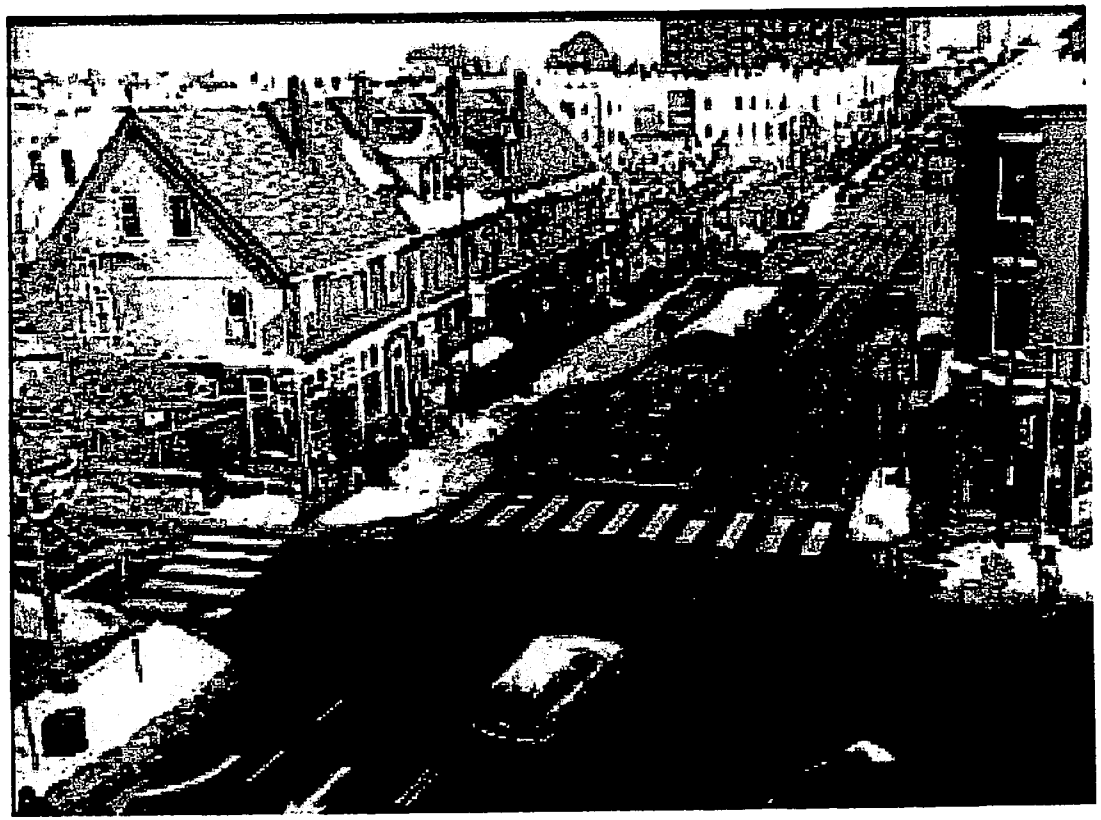


INMAN SQUARE
"DIGITAL ZOOM"



INMAN SQUARE
"ANALOG ZOOM"

INMAN SQUARE
"HOME VIEW"



How will use of the system be controlled?

- Access to the system is permissions based. F example, a public safety dispatcher may have "view only" access to the camera's home view and the Shift Commander for the Police Department may have the ability to pan, tilt, zoom and capture images.
- The system logs all activity – time, date, and activity performed by a user
- A draft policy covering acceptable use has developed and will be implemente Cambridge agency acce

How will we control access by other communities?

- Access to Cambridge cameras will be via a Memorandum of Understanding.
- Outside Metro Boston communities will only have the ability to view the camera – they will not be able to control the camera

Other potential benefits from the CIMS network:

- Ability to monitor cameras of surrounding communities on our borders (ie, Linear Park on the Somerville border)
- Saved expense from eliminating some Verizon landlines currently used for radio traffic
- Potential to add "wireless" call boxes in the vicinity of installed cameras
- Potential to create a backup Voice over IP (VoIP) telephone system between the Metro Boston communities for use during emergencies

B

A Statement by Nancy Murray, Education Director of the ACLU of Massachusetts, before the "Civic Unity" hearing of the Cambridge City Council

January 22, 2009

I am a Cambridge resident (204 Erie Street) and Director of Education at the ACLU of Massachusetts, which has 1300 members in Cambridge. We have many concerns about the DHS-funded surveillance cameras being installed in Cambridge.

As we understand it, the eight surveillance cameras purchased for Cambridge are part of a "Urban Area Security Initiative" grant worth $4.6 million from the US Department of Homeland Security. The camera network linking Cambridge and 8 other Greater Boston communities (including Brookline and Somerville) will be run out of the Office of Emergency Preparedness in Boston. Cambridge will thus be incorporated into a rapidly growing network of surveillance cameras across the country funded by the DHS in the name of "fighting terrorism." Even Liberty, Kansas – population 95, now has a DHS-funded surveillance camera.

This raises a host of questions. Whose eyes will be watching us as we go about our daily business? Will the digital images be shared – if so, with what agencies and on what terms? Where will they be stored and for how long? Who will have access to them? Will they, like so much other public and private data be transmitted to the secretive Commonwealth Fusion Center and possibly be used for data mining purposes? The Fusion Center in Maynard, Massachusetts is now one of 66 Fusion Centers in the country which are emerging as hubs of a new domestic intelligence apparatus that collects information about crime, everyday activities, personal relationships, and tips from the public about suspicious activity, and uses data mining techniques to identify individuals for closer scrutiny, all without any independent oversight.

These questions about the collection, storage, sharing and use of data raise serious concerns about privacy, the surveillance of lawful First Amendment activity, and the nature of a free society. We are alarmed to learn that these extremely powerful cameras will be placed at two sites in Cambridge where demonstrations and vigils often take place – namely, Holyoke Center in Harvard Square and Central Square.

Existing studies show how easily the cameras can be abused. In Britain, police officers assigned to monitor surveillance cameras ended up using them to zoom in on women's body parts and even stalk women. They have also been used to target and track people of color. Their round-the-clock monitoring can make immigrants in our community feel even more vulnerable. The potential to use cameras for racial, ethnic or religious profiling is especially troubling because of three recent developments:

• A report in the December 9th *Cambridge Chronicle* that Cambridge police officers recently went to Israel along with local officials from the FBI and state police to study Israel's counter-terrorism methods. Racial profiling is fundamental to Israel's security strategy, as the US State Department itself has recognized.

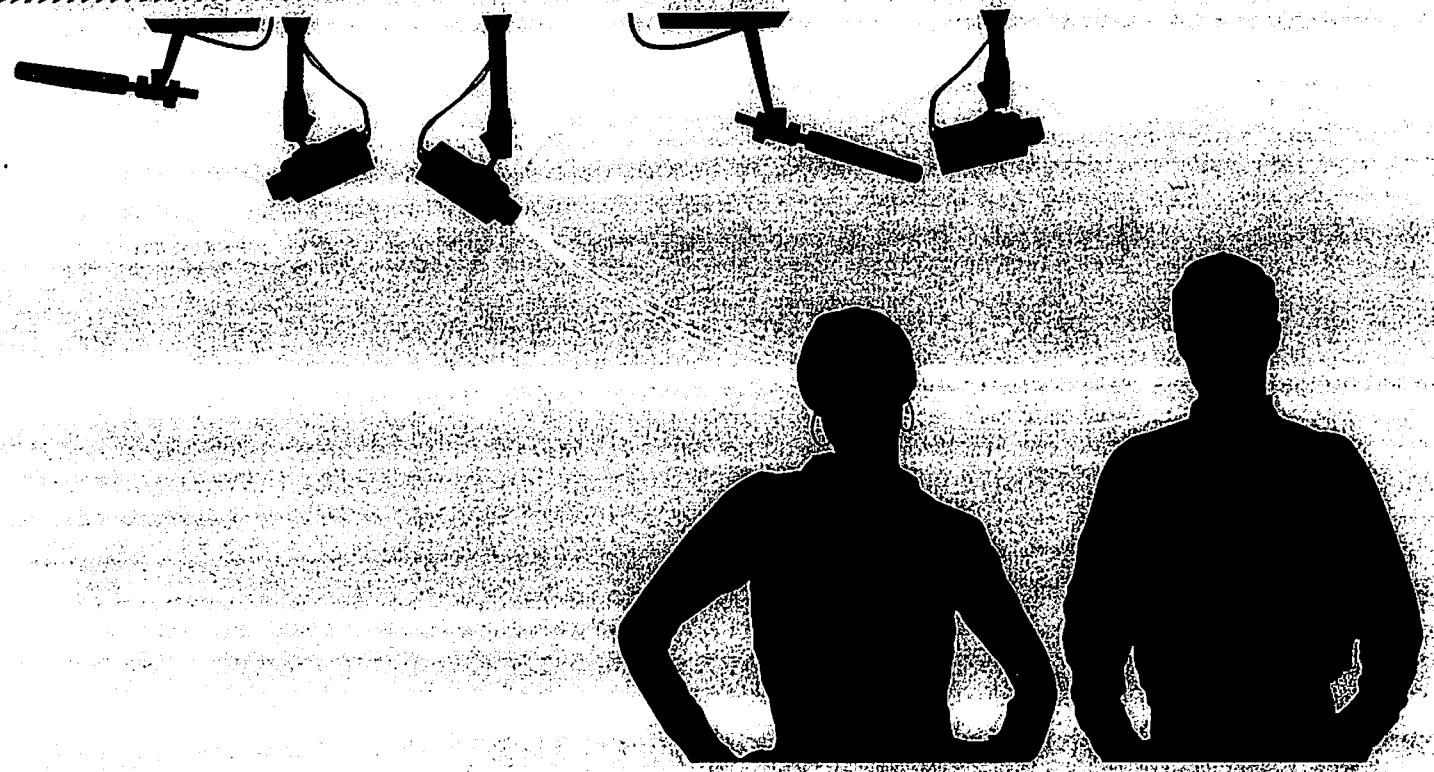
• New FBI guidelines that permit agents to track people based on their race and ethnicity, without the standard of "suspicion" required by the Fourth Amendment.

• Reports in the *Wall Street Journal* (June 13 and November 13, 2008) listing Boston - the hub of this surveillance camera network - as one of nine cities and states across the country which will soon follow in the steps of the LAPD and train police officers to identify and file suspicious activity reports on 65 different behaviors that could "relate to terrorism" - an example given is taking pictures of a building. This information will reportedly be deposited in state fusion centers, and made available to the DHS, FBI and security officials around the country. The *Wall Street Journal* reports that the next stage is getting the public involved "in an education program, called iWATCH, which will instruct citizens on specific behaviors to report to authorities" (*Wall Street Journal*, November 25).

Whether or not iWATCH comes to the Urban Area Security region of which Cambridge is a part, I don't think it is farfetched to assume that eventually cameras could be equipped with software to track specific behaviors, with that data being deposited in the fusion center. We know from experience with the bloated and deeply flawed "No Fly Lists," that once false or misleading information lands an innocent person in one of these mega databases, that person may be stuck in there forever with all kinds of harmful consequences – unless his name is Edward Kennedy.

In conclusion, I thank Councilor Decker for initiating this discussion which is really about the kind of society and community we want to live in. Like President Obama, who in his inauguration speech said "we reject as false the choice between our safety and our ideals," the ACLU believes that we can maintain both our safety and our freedom. As you will shortly be hearing, evidence shows that surveillance cameras are not effective in fighting crime and in ensuring a safe evacuation in case of a catastrophic event. So let us not be misled by what is indeed a false choice in this case, and instead preserve Cambridge as a city in which our ideals can flourish — a community where immigrants feel welcome, where diversity and First Amendment activity can thrive and where privacy rights are respected.

C



UNDER THE WATCHFUL EYE

By Mark Schlosberg and Nicole A. Ozer
THE CALIFORNIA ACLU AFFILIATES

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY

PART I
3 THE IMPACT OF VIDEO SURVEILLANCE CAMERAS ON CIVIL LIBERTIES

PART II
11 SURRENDERING PRIVACY DOES NOT MAKE US SAFER

PART III
16 PUBLIC RECORDS SURVEY AND FINDINGS

PART IV
18 RECOMMENDATIONS AND CONCLUSION

20 ENDNOTES

AUTHORS: Mark Schlosberg, Police Practices Policy Director, and Nicole A. Ozer, Technology and Civil Liberties Policy Director with the American Civil Liberties Union of Northern California.

CONTRIBUTING WRITERS: Peter Bibring, Staff Attorney ACLU of Southern California, and Lauren Woon, Program Assistant ACLU of Northern California.

RESEARCH ASSISTANTS: Joyce Bradberg, Lara Hoffman, William Reagon, Fatima Silva, Jennifer Turner, and Alison Watkins assisted with this project.

EDITORS: Cathy de Heer and Rene Ciriacruz

DESIGN: Chen Design Associates **LAYOUT:** Gigi Pandian **PRINTING:** Inkworks Press

EXECUTIVE SUMMARY

Across the country extensive media coverage, litigation, and congressional debate have targeted domestic surveillance programs operated by the Department of Defense, the FBI, and the National Security Agency (NSA). Until recently, however, very little attention and public debate had been directed at the dramatic expansion in government video surveillance of public space at the local level.

This report explains in detail the joint assessment of the three California ACLU affiliates of government-funded video surveillance cameras and the current state of video surveillance in California: Part I looks at the threat posed by public video surveillance to privacy and other civil liberties. Part II examines law enforcement justifications for video surveillance programs and an evaluation of these programs' effectiveness. Part III reviews the findings from our public records survey. Part IV offers policy recommendations.

THREAT TO CIVIL LIBERTIES FROM COMBINED TECHNOLOGIES

Government-run video surveillance can radically alter the relationship between law enforcement and the public. By itself, pervasive video surveillance threatens privacy rights. But even more disturbing, the threat multiplies when government combines cameras with emerging technologies such as automated identification software, face and eye scans, radio frequency identification (RFID) tags, and databases accessible to law enforcement. In that context, video surveillance provides a critical pillar of a surveillance infrastructure. It creates the potential for the government to monitor people in public space, in a way envisioned only in futuristic novels.

GOVERNMENT FUNDING FOR SURVEILLANCE CAMERAS

Video surveillance cameras are a familiar sight at automated banking machines and other private businesses, but government-funded camera systems in public spaces are a recent development. Some jurisdictions experimented with surveillance systems in the 1990s, but several cities eventually rejected the systems because of their cost, ineffectiveness, and impact on civil liberties.[1]

However, the events of September 11, 2001, radically changed perspectives toward privacy and security and there is now a homeland security bureaucracy that is flush with money and eager to support the efforts of local governments to adopt new surveillance

technology. The Department of Homeland Security has offered hundreds of millions of dollars in grants to local governments for video surveillance cameras and systems.[2]

While the federal government has been handing out money for new surveillance systems, cities and counties throughout California are grappling with the very real problem of violent crime in their communities. Residents facing rising homicide rates have demanded solutions from police departments and elected officials.[3] Security companies have engaged in active marketing to capitalize on general concerns about safety and on the resources available since September 11. Seeing new opportunities to address the public's fears—and using Department of Homeland Security funding in some cases—the local government has responded, in part, by installing surveillance camera systems.

CAMERAS NOT PROVEN EFFECTIVE; NO SAFEGUARDS AGAINST ABUSE

Residents in high-crime areas, their political leaders, and police officials often see surveillance systems as an obvious solution to crime. Often, however, little consideration is given to the significant evidence demonstrating that camera surveillance is ineffective, especially when compared with other alternatives. Even less consideration is given to the expanded surveillance infrastructure's long-term impact on privacy and on the relationship between the government and the people. Cities throughout California have approved and implemented camera systems without guidelines to guard against abuse and, in most circumstances, with little or no public debate.

ACLU PUBLIC RECORDS SURVEY ON VIDEO SURVEILLANCE

As the media began reporting on the proliferation of surveillance systems, the ACLU began investigating the extent of video surveillance in California. We conducted a public records survey of 131 jurisdictions throughout the state. Among the key findings:

- 37 cities have some type of video surveillance program
- 18 cities have significant video surveillance programs of public streets and plazas; an additional 10 jurisdictions are actively considering such expansive programs
- 18 cities have systems in which police actively monitor the cameras
- Only 11 police departments have policies that even purport to regulate the use of video surveillance cameras
- No jurisdiction has conducted a comprehensive evaluation of the cameras' effectiveness

As cities throughout California move quickly to approve and install video surveillance, we strongly urge local governments to pause and consider the impact of these systems. Surveillance cameras will not improve public safety, and limited funds can be better spent on programs that are both proven effective and less invasive, such as improved lighting, foot patrols, and real community policing.

As former Oakland Mayor (now California Attorney General) Jerry Brown said in 1999 when the City of Oakland rejected proposed video surveillance cameras: "Reducing crime is something the community and police must work on together. Installing a few or a few dozen surveillance cameras will not make us safe. It should also not be forgotten that the intrusive powers of the state are growing with each passing decade."[4]

MIKE RHODES

Help from DHS: The Department of Homeland Security gave Fresno a large grant for surveillance cameras.

PART I

THE IMPACT OF VIDEO SURVEILLANCE CAMERAS

ON CIVIL LIBERTIES

> "Reducing crime is something the community and police must work on together. Installing a few or a few dozen surveillance cameras will not make us safe. It should also not be forgotten that the intrusive powers of the state are growing with each passing decade."
>
> — Oakland Mayor Jerry Brown, 1999

George Orwell's novel, *Nineteen Eighty-Four,* painted a picture of a world without privacy, in which government authorities, using a wide array of technologies, continuously monitored human activity. The loss of privacy shaped society, enabling government to control all aspects of people's lives.

Orwell wrote at a different time and in a different political context, when the fear of communism and totalitarianism was real and widespread. However, there are strong parallels between the society he described and the conditions increasingly made possible by the U.S. government's growing surveillance capabilities. Instead of communism, the public now fears terrorism and gun violence, and although government surveillance is not yet pervasive in the United States, reality is not very far from fiction.

In recent years, the government has dramatically expanded its surveillance capabilities through the proliferation of government-funded camera systems in public spaces. On its own terms, pervasive video surveillance threatens privacy and other constitutional rights. The threat multiplies when surveillance cameras are combined with other emerging technologies such as automated identification software, face and eye scans, and radio frequency identification (RFID) tags. In that context, video surveillance provides a critical pillar of a surveillance infrastructure and creates the potential for the government to monitor people in public space in a way previously envisioned only in futuristic novels. It is particularly troubling that while the technology has improved along with the government's ability to infringe on constitutional rights, the legal landscape has not kept pace.

VIDEO SURVEILLANCE CAMERAS

Video surveillance has doubled in the last five years: It is now a $9.2-billion industry, and J. P. Freeman, a security industry consultant, estimates that it will grow to $21 billion by 2010. He predicts that "pretty soon, cameras will be like smoke detectors: They'll be everywhere."[5]

Cities across the country are jumping on the surveillance bandwagon. In Chicago, Mayor Richard M. Daley has announced that he wants the city to have a camera on almost every corner by 2016. Not all of these cameras are government-funded and controlled—large numbers are privately owned surveillance cameras. Even the private cameras, however, contribute to the overall expansion of government surveillance because the government can ask businesses for access to video footage.[6]

Government surveillance camera programs pose several grave threats to civil liberties. First, these programs have a significant impact on privacy. Twenty-four-hour video monitoring of public spaces gives the government a vast quantity of information on private citizens that would otherwise be unavailable, allowing it to monitor people engaging in wholly innocent and constitutionally protected behavior.

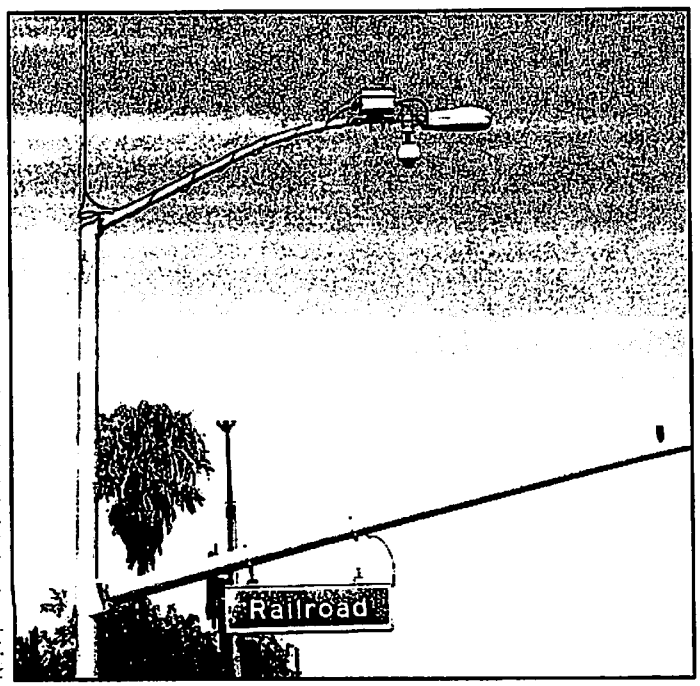
Moreover, the technological sophistication of new camera systems adds an entirely new dimension to surveillance. These cameras do not produce the grainy footage of yesteryear. Many of these state-of-the-art systems—perched atop utility poles with 360-degree views, rolling 24 hours a day—generate DVD-quality video footage, and some have the capability to record sound.[7] They can zoom in close enough to show the title of 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.[8] Everything a camera sees or hears can be stored in perpetuity on its hard drive or in a central database.

OTHER SURVEILLANCE TECHNOLOGIES: AUTOMATED IDENTIFICATION SOFTWARE, FACE AND EYE SCANS, AND COMPUTER-READABLE TAGS

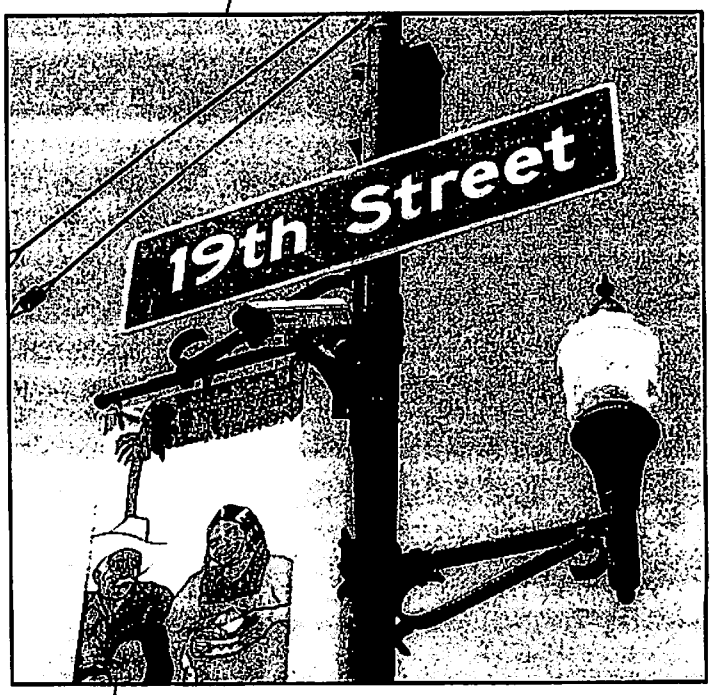
The threat to civil liberties multiplies when cameras are used in combination with other surveillance technologies. Recently developed software can monitor camera feeds—automatically classifying objects, tracking recorded movement, and classifying certain behavior as "suspicious activity."[9]

Such software was recently installed in the San Francisco International Airport as part of a $30-million pilot program funded by the federal government.[10] In response to privacy concerns, the owner of the software company dismissed worries, saying: "With the world of intelligent video we will only be recording suspicious behavior . . . We won't be recording you walking down the street."[11] Technology used in one context, however, can quickly expand to other uses. Industry consultants already hope to sell surveillance software for both government and commercial uses.[12]

It is not far-fetched to think that face recognition technology will soon be used to connect camera footage with other images



KATE KENNEDY, DAVID FAMY RHINE



KATE KENNEDY, TAMMY RHINE, AND JULIANA PEARSON

Pittsburg (left) and San Francisco (right) have recently initiated camera programs and have plans for more.

HISTORICAL IDEAS ABOUT SURVEILLANCE & THEIR MODERN-DAY APPLICATIONS

The concept of using surveillance to deter crime and achieve a level of social control is not new. Sociologist Jeremy Bentham developed the theory in the late 18th century and it is best represented by his concept of a "Panopticon," a model prison where prisoners could be observed, but they could not see who was watching and tell when they were being watched. "The psychological objective of such a system was that the subjects of surveillance would believe that their only logical option was to conform. Thus each individual would become their own overseer."[13]

Two centuries later, this concept of surveillance was extended beyond the walls of the prison and out into society. Michel Foucault in 1977 argued that the mechanism and principles used to control prisoners in Bentham's Panopticon could be similarly applied to citizens throughout society.[14] Orwell also elaborated on that idea in chilling detail: "Every citizen, or at least every citizen important enough to be worth watching, could be kept for twenty-four hours a day under the eyes of the police."[15]

When *Nineteen Eighty-Four* was published in 1949, Orwell's tale seemed far-fetched. Futuristic films from recent years such as "Minority Report" and "Gattaca" still appear fanciful, but the concepts and theories these stories illustrate have started to be put into practice. Within the last decade, the installation of surveillance cameras on public streets and in public parks has extended the eye of government into the public's daily life. What is more, video surveillance is being combined with other technologies, such as face recognition, to expand government monitoring of the public even further.

and information about people. In fact, the Los Angeles Police Department was field-testing face recognition software in November 2006.[16] By combining video footage with face recognition software, the government could quickly identify individuals walking down a street, participating in a political rally, or entering a doctor's office.

Technology also exists for identifying a person by using a scan of the retina, and a patent has been filed for a device that can scan the iris of someone's eye from a distance.[17] Like a fingerprint an iris is unique, so the image can be used to identify an individual. Combining iris scanners with surveillance cameras would give the government another way to identify people in public without their knowledge or consent.

Another surveillance technology called radio frequency identification (RFID) could also be coupled with video surveillance cameras, enabling the government not only to record images, but also to capture detailed information on anyone who came within the cameras' range.[18] RFID tags are tiny computer chips that can be embedded in identity cards and other items. Whatever personal information is encoded on the chip, such as a name, address, or digital photograph, can be read by a machine at a distance of many feet without alerting the holder of the identification document.[19] The State Department has already embedded RFID tags in all new U.S. passports and the Department of Homeland Security is considering its use in other travel documents and identification cards.[20] With RFID tags embedded in identity cards and machines to read them integrated into public surveillance cameras, government would be able to collect and compile an immense amount of information about individuals and their private lives.[21]

THE REAL ID ACT AS ENABLER OF SURVEILLANCE TECHNOLOGIES

Automated identification technology, such as facial recognition and iris scans, are not currently used by many local jurisdictions because they are expensive, technologically limited in their efficiency, and the government currently does not have digital photographs and biometric information on file for most people. However, unless pressure from the states and civil liberties groups succeeds in stopping implementation of the federal Real ID Act, the federal government will establish such files—a nationwide database of information on every U.S. citizen—in the next few years.

As technology has improved, so has its ability to infringe on constitutional rights. It is the legal landscape that has not kept pace.

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. Under the Act, a state driver's license is not acceptable for boarding a plane, opening a bank account, or entering a federal facility unless it complies with Department of Homeland Security standards for uniformity: every license must carry the driver's photograph and all the personal information on it in a digital format that can be read by any state or federal computer across the country. All this data will then be accessible, through a shared database, to law enforcement agencies in all 50 states and to the federal government.[22] A biometric identifier, such as a scan of the iris or retina, could also be required on the new driver's license.[23]

This combination of video cameras and other surveillance technologies—face and iris scanning, national identity cards, and RFID tags—will enable the government to confirm the identity of any passerby and gain access to a wealth of personal information. In the future, this information could include not only the data in the RFID tag itself—name, address, photo, and any biometric scans—but also anything else that might be linked to a person in a national database. It might include, for example, your motor vehicle records, police records, employment history, DNA and drug testing records, and you and your family's travel and buying habits.[24]

MULTIPLE CONSTITUTIONAL PROTECTIONS THREATENED

As technology has improved, so has its ability to infringe on constitutional rights. It is the legal landscape that has not kept pace. Video surveillance systems are proliferating despite the fact that they infringe on the freedom of speech and association guaranteed by the First Amendment and threaten the anonymity and privacy protected by the Fourth Amendment and state constitutions. Anonymity and privacy are both independent rights and also function to safeguard speech rights.

THE RIGHT TO FREEDOM OF SPEECH, ASSOCIATION, AND MOVEMENT

People tend to have much less confidence in their overall freedom to act, speak, and associate with other people or groups when they know they are being watched. Think of an innocent activity such as dancing at a wedding or party: Many people would wait until others were already dancing and the lights were turned low, so that they would be less visible to onlookers. As one legal scholar noted, "No matter how innocent one's intentions and actions at any given moment . . . persons would think more carefully before they did things that would become part of the record.[25] Once people know they are being "observed and recorded, their habits change; they change."[26]

Moreover, with a public video surveillance camera it is not just anyone watching—it is the government watching.

The right to express oneself not just through action, but also in the choice to stay still or "repose" has been continually affirmed by the U.S. Supreme Court. In *Chicago v. Morales*, the Court wrote that

> freedom to loiter for innocent purposes is part of the "liberty" protected by the due process clause of the Fourteenth Amendment . . . Indeed, it is apparent that an individual's decision to remain in a public place of his choice is as much a part of his liberty as the freedom of movement inside frontiers that is "a part of our heritage," or the right to move "to whatsoever place one's own inclination may direct."[27]

Professor Jeffrey Rosen studied the British video surveillance system and found that cameras cause individuals to censor themselves, concerned that engaging in certain activities, or even lingering in public spaces could draw the attention of law enforcement. He concluded that "rather than thwarting serious crime, the cameras are being used to enforce social conformity in a way that Americans may prefer to avoid."[28]

There is little doubt that when people know a camera is aimed at them, they worry about who might be watching, what others are thinking, and how the pictures might be used—or misused. In a public context, video cameras deter people from engaging in activity that is both perfectly legal and constitutionally protected.[29]

ANONYMITY AS A SAFEGUARD FOR FREEDOM OF SPEECH AND ASSOCIATION

Video cameras in public places also chill speech and associational activity by preventing people from remaining anonymous. Installing cameras in public spaces is tantamount to requiring people to identify themselves whenever they walk, speak, or meet in public. If these surveillance systems were everywhere, it would be practically impossible to be in a public place without wondering whether the government was monitoring and recording who you were, where you were, and what you were doing. A government camera aimed at the entrance to a building where an organization held meetings could reveal association as readily as a membership list.[30]

Such a scenario would violate established First Amendment protections of speech and association. The U.S. Supreme Court has held that requiring people to identify themselves when expressing themselves in public is unconstitutional; likewise for requiring identification of a person's association with others or with organizations. Individuals have a right to protest, leaflet, and circulate petitions anonymously,[31] and courts have also ruled that it is improper to force the disclosure of membership lists.[32]

Furthermore, courts have ruled that surveillance that targets individuals, intimidates them, or discourages attendance at an organizational activity or membership in an organization is an improper infringement on free speech and the right of association.[33] As U.S. Supreme Court Justice John Paul Stevens commented in *McIntyre v. Ohio Elections Commission*, wherein the Court found it unconstitutional to prohibit the distribution of anonymous campaign literature, "(t)he decision in favor of anonymity (is) motivated by fear of economic or official retaliation, by concern about social ostracism, or merely by a desire to preserve as much of one's privacy as possible . . . (it) is an aspect of freedom of speech protected by the First Amendment."[34]

THE RIGHT TO PRIVACY

In addition to protecting the right to freedom of speech and association, privacy has an independent value in freeing people from government intrusion unless there is sufficient justification for it. The Fourth Amendment protection against unreasonable search and seizure guarantees this right to privacy, and so does the privacy amendment in the California Constitution. Recent court decisions, however, have not kept up with technology's potential for abetting government in violating these rights.

Fourth Amendment. The Fourth Amendment promises all Americans a zone of control around their bodies and possessions that the government cannot enter without reasonable cause. This zone of control extends far beyond the front door of a home; it may, under appropriate circumstances, even extend to places or things that a "person seeks to preserve as private, even in an area accessible to the public."[35] A person is entitled to protection if a court finds he has a "reasonable expectation of privacy."[36]

Video surveillance cameras do not simply record information that is readily observable or available (see "Other Surveillance Technologies: Automated Identification Software, Face

POLICE ACCESS TO PRIVATE SECURITY CAMERAS

In the age of the Internet, cities do not even need to install their own cameras to engage in video surveillance. In Corona, Calif., the city's Web-Watch program gives police Internet access (through a user name and password) to live "feeds" from the video systems of participating businesses. Officers at the Corona Police Communication Center can view what the cameras are recording and can even pan, tilt, and zoom the cameras remotely.[37]

The system is intended for responding to alarms and calls for service and to reduce responses to false alarms. But nothing in either the Web-Watch contracts or city policies restricts the police to viewing security feeds only when an emergency call is made. Nothing prevents the city from monitoring video feeds for any purpose at all. In fact, the city does not even face liability for abuse, because participating businesses must explicitly agree to indemnify the city against liability for invasion of privacy or recording of unauthorized communications.[38]

Other California cities with public-private hybrid programs include Brentwood and Oakland, where redevelopment money has been used to fund a small number of cameras for local businesses.[39]

and Eye Scans, and Computer-Readable Tags," page 5), they also record additional information and retain it for uses never before possible. Regrettably, the courts' view of the privacy protections that apply in public places have not expanded to account for this change in the technological landscape, and Fourth Amendment court decisions do not reflect it. As technology advances, individuals must demand that privacy rights are not left behind, and courts must be persuaded to take a more nuanced view of what is meant by a "reasonable expectation of privacy."

California Privacy Amendment. Widespread use of video surveillance is also inconsistent with the explicit right to privacy in the California Constitution. Overwhelmingly approved by voters in 1972, the amendment was specifically designed to guard against "the proliferation of government snooping and data collecting that is threatening to destroy our traditional freedoms."[40] In *White v. Davis* in 1975, the first California Supreme Court decision 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.[41]

Video surveillance cameras and other surveillance technologies present just the type of "modern threat" the amendment was meant to guard against.

MODERN TECHNOLOGICAL AND LEGAL FACTORS THAT AFFECT PRIVACY

Personal information captured by surveillance cameras is at risk through both lawful public access and theft on the networks over which it travels. Many cities rely on wireless Internet systems to handle footage from surveillance cameras. These systems control the cameras remotely and transmit images to police stations and individual squad cars. Technological vulnerabilities in wireless networks drastically compound the privacy risk by making it possible for anyone to break into the system to control the cameras and gain access to the footage.

PRIVACY DOES NOT END AT THE FRONT DOOR

The police cannot stop and search a person for no reason on a public street.[42] A public telephone cannot be tapped without a warrant.[43] People cannot be forced to give their names before they distribute leaflets.[44] These limits on government power hold because the right to privacy and free expression extends far beyond a person's front door.

"People are not shorn of all Fourth Amendment protection when they step from their homes onto the public sidewalks." U.S. Supreme Court in *Delaware v. Prouse*, 1979.[45]

"What a person seeks to be private, even in an area accessible to the public, may be constitutionally protected. " U.S. Supreme Court in *Katz v. United States*, 1967.[46]

"Streets and parks . . . have immemorially been held in trust for the use of the public and, time out of mind, have been used for purposes of assembly, communicating thought between citizens, and discussing public questions. Such use of the streets and public places has, from ancient times, been a part of the privileges, immunities, rights, and liberties of citizens." U.S. Supreme Court in *Hague v. CIO*, 1939.[47]

Privacy and freedom of expression in public places are the values on which American society was forged. Without them, it would be very difficult to speak freely, join and support causes, and assemble to criticize government and safeguard democracy. People have a right not only to engage in speech and protest on public streets, but also to do so anonymously so that they can speak without fear of reprisal from the government.[48] This right to anonymity, or namelessness, is necessarily tied to privacy. A person cannot remain anonymous if personal information and identity do not remain private.

Video surveillance cameras may make it easier for the government to identify people in public, but that does not make video surveillance acceptable.

> "I'm really concerned about what happens to the product of these cameras, and what comes next? [A]re we really moving towards an Orwellian situation where cameras are at every street corner? I really don't think that's the kind of country that I want to live in."
> —Ian Readhead, Deputy Chief Constable of Hampshire, England

WIRELESS SYSTEMS

Wireless networks send information through radio waves in the air. Just as someone using a police scanner could hear what police are transmitting through their in-car radios, someone with a computer and an incentive to break into a video surveillance system on a wireless network could intercept the video data. Wireless networks are extremely vulnerable to unauthorized access, even when the data transmitted is "encrypted" (that is, encoded to keep it private). Tools for breaking into wireless systems are "freely available on the Internet,"[49] and it is easy for thieves to pick up the 2.4 GHz radio frequency on which video surveillance footage most often travels.[50]

In Northern California, the town of Brentwood has a wireless network that enables the police department to use and control cameras remotely from patrol cars. The little town of Ripon in the San Joaquin Valley, with a population of fewer than 11,000 people, has installed a municipal wireless system that transmits data among 20 surveillance cameras.[51] The wireless network proposal presented for San Francisco in 2006 touted the network's ability to support the city's new video surveillance infrastructure.[52] Sacramento is also in the process of developing a municipal wireless system and has plans to connect hundreds of cameras to create one large surveillance system that can be used and controlled remotely. Across the country, more than 300 municipalities are considering offering public wireless Internet access, and vendors have seized on the use of those networks to facilitate public video surveillance as a significant selling point.[53]

PUBLIC RECORDS LAW AND MANDATORY ACCESS TO VIDEO FOOTAGE

The ACLU has always strongly supported public access to government records, and under the California Public Records Act, records held by the government are presumed open and subject to narrow exceptions, including records related to a criminal investigation.[54] Under the Act, video surveillance footage generated by government surveillance cameras would almost certainly be accessible to the public. In fact, at least one jurisdiction—the city of Fresno—has a policy acknowledging that some video footage is accessible to the public.[55]

The implications of public access to video surveillance footage are broad and generally have not been considered by policy-makers. Anyone can request and gain access to video footage from any location where a camera has been deployed, for a whole host of invasive reasons. For example, an untrusting husband or wife might want to see if a spouse was entering or exiting a home or business that happened to be in range of a camera; an opposing political candidate might want to see people entering and leaving an opponent's campaign headquarters; or a political organization might want to identify members of the opposition who happened to attend a rally within eyeshot of a camera.

The public should have access to the same information as the government; however, such access also means that widespread video surveillance systems can quickly prevent people from keeping their activities private, not just from the government, but also from other private parties.

DISCRIMINATORY AND ABUSIVE USE OF CAMERAS

Finally, in addition to privacy concerns, the potential for misuse of video surveillance systems raises significant equal protection issues. Studies published in Great Britain have shown discriminatory use of surveillance cameras.[56] 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 10 women was "targeted for entirely 'voyeuristic' reasons by male operators," and that "40 percent of people were targeted for 'no obvious reason,' mainly 'on the basis of belonging to a particular sub-cultural group.'"[57]

The British reports were not anomalous. In the United States, a number of abuses involving surveillance cameras have been reported in the last few years, ranging from the surveillance of demonstrations to the targeting of women and minorities. A San Francisco police officer in 2005 faced disciplinary action for using surveillance cameras at the airport to ogle women.[58] According to a recent evaluation of surveillance camera systems by a scholar at the Naval Postgraduate School in Monterey, Calif.,

> With more than 1 million closed-circuit television (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.[59]

RAPID GROWTH OF VIDEO SURVEILLANCE IN GREAT BRITAIN: A CAUTIONARY TALE

Great Britain provides the clearest example of how small surveillance systems can rapidly mushroom into comprehensive government monitoring schemes. There, video cameras are already much more pervasive than in the United States. Following two bombings in the early 1990s by the Irish Republican Army, the beginnings of a surveillance system were established in London.[60] Seventy-nine British cities, by 1994, were monitoring their central districts with surveillance cameras, and by 1998 three-quarters of the Home Office's crime prevention budget was being spent on cameras.[61] By 2004 approximately 500 towns and cities had surveillance systems, with more than four million cameras being used and operated throughout Great Britain—one for every 14 people. In London the average person is now captured on video camera 300 times a day.[62]

This rapid proliferation of cameras is just one aspect of the surveillance infrastructure in Great Britain; more expansion is planned. The Home Office is investing significant resources on efforts to improve face recognition technology and plans to use it widely by 2016.[63] British law enforcement is also using cameras on highways to capture license plate numbers and track driving patterns over a CCTV network.[64]

Camera systems are also becoming more invasive. Some cities are considering attaching microphones to cameras designed to "pick up aggressive tones on the basis of 12 factors including decibel level, pitch, and the speed at which words are spoken."[65] In the town of Middlesbrough, seven of 158 cameras have loudspeakers attached so that control room operators can speak to people passing by, issuing alerts such as "Warning—you are being monitored by CCTV."[66]

Great Britain started out with a small pilot program in just three towns.[67] Just 15 years later, the country has taken on significant characteristics of a Big Brother society, and even police are now expressing concern. According to Ian Readhead, Deputy Chief Constable of Hampshire, "I'm really concerned about what happens to the product of these cameras, and what comes next? If it's in our villages, are we really moving towards an Orwellian situation where cameras are at every street corner? I really don't think that's the kind of country that I want to live in."[68]

This story shows how fast small programs can expand into large ones. It is a warning for local governments and communities to stop and think before starting down the path of video surveillance.

PART II

SURRENDERING PRIVACY
DOES NOT MAKE US SAFER

Concern about crime and the belief that surveillance cameras make communities safer overshadow video surveillance's corrosive impact on civil liberties. Crime is a very real problem in many communities, with both residents and police strongly motivated to do something about it. However, video surveillance is not the solution.

Numerous studies of existing camera programs demonstrate that they do not significantly reduce crime, especially violent crime in city centers. Furthermore, expectations that surveillance cameras will significantly increase the success rate of criminal prosecutions have not been met.

Instead, within limited public-safety budgets, surveillance cameras come at the expense of proven crime reduction measures such as better lighting, foot patrols, and community policing. In this sense, throwing money at video surveillance actually detracts from law enforcement's efforts to reduce crime.

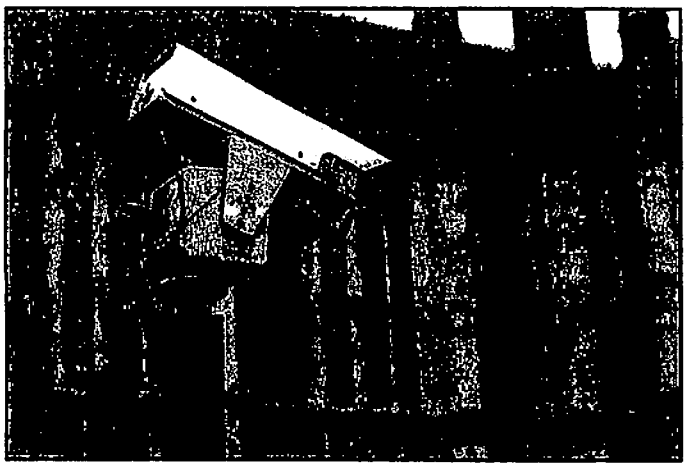
STUDIES FAIL TO SHOW VIDEO SURVEILLANCE DETERS CRIME OR REDUCES FEAR OF CRIME

Crime Rates Not Reduced By Cameras

Law enforcement agencies justify video surveillance programs mainly by claiming that they deter criminals. Cameras are being touted as a crime prevention tool in places all over California. For example, in Brentwood police claim that cameras serve "as an effective deterrent to robberies and burglaries . . . They are definitely a deterrent and they help in apprehending suspects in criminal activity";[69] in Clovis police say the cameras will "enhance public safety though prevention as potential criminals realize that the police utilizing remote cameras are monitoring them";[70] and in Indio the police department has begun deploying mobile cameras "to deter vandalism and other criminal activity."[71] In San Francisco local law requires a finding of "potential deterrence" before cameras can be placed.[72] Indeed, residents of high-crime communities sometimes seek to install cameras in hopes of making their neighborhoods safer.

However, though it may seem intuitive to policy-makers or concerned residents that video surveillance cameras will reduce crime, studies suggest otherwise.

In Great Britain, where camera systems have been in place for close to a decade, criminologists have conducted a number of studies to review their actual impact. A 1999 study by the Scottish Central Research Unit evaluated crime statistics before and after the installation of surveillance cameras in Glasgow, Scotland. There, researchers found reductions in crime "no more significant than those in control areas without the camera locations."[73]



While cameras like these blanket Great Britain, they have not prevented terrorist attacks and studies show they have failed to significantly reduce crime in city centers.

A broader study by the British Home Office in 2002 looked at the cameras' effects on crime in 18 different jurisdictions. The survey found reductions in vehicle crimes in certain areas—particularly parking garages—but found no significant impact on violent crime: "In the city centre and public housing setting, there was evidence that CCTV led to a negligible reduction in crime of about 2 percent in the experimental areas compared with the control areas."[74] Yet these are the very areas where many jurisdictions (such as San Francisco and Los Angeles) are deploying cameras.

The most recent comprehensive study, by Martin Gill and Angela Spriggs of the University of Leicester in England, evaluated 13 systems in Great Britain and reached similar findings. Although the British government spent millions of dollars on the systems, these have not had a significant impact on crime. In some areas crime increased and in others it decreased. In comparison 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.[75]

Fear of Crime Not Reduced By Cameras

According to the British studies, not only did cameras fail to decrease the actual rate of crime, they also failed to reduce the fear of crime. In the Glasgow study, researchers found that installing cameras did not make people more comfortable venturing into high-crime areas.[76] The Gill and Spriggs study, in fact, 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.[77]

Criminals Not Deterred By Cameras

The failure of cameras to reduce crime (or fear of crime) is also reflected in how offenders view video surveillance. Two studies conducted in the United States in 1985 by the Athena Research Corporation surveyed 181 armed robbers in prisons in New Jersey, Texas, and Illinois, and an additional 310 armed robbers in 20 state prisons in Maryland, Texas, and Washington. The researchers asked about offender planning, methods, and motives, seeking to determine what means were most effective in deterring crime.[78]

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."[79]

A third offender survey, conducted in Great Britain in 2003, reached similar conclusions. The researchers interviewed 77 convicted male offenders who had committed a prior theft or fraud. Again, the 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."[80]

HOW TO LOOK AT CAMERAS' EFFECTIVENESS

Law enforcement may report a drop in crime in an area directly under surveillance by a video camera, but such a statistic reveals little about whether the camera caused the reduction in crime or whether crime simply moved out of camera range without actually decreasing at all. To conduct a comprehensive evaluation, a jurisdiction must, at a minimum, look at the following information:

1. Crime at the camera location before and after placement of the camera
2. Crime within 500 feet and 100 feet of the location before and after placement
3. Overall crime within the jurisdiction
4. Other changes that might account for reductions in crime

Despite the relative simplicity of such a study and the millions being spent on new camera systems, not one jurisdiction in our survey (see Section III) had studied the effectiveness of surveillance cameras after they were put in place.

Even in the face of this evidence, law enforcement and government officials in California continue to claim that cameras deter crime. In San Francisco, for example, the Director of the Mayor's Office of Criminal Justice admitted, at a public hearing on the proposed expansion of the city's video surveillance program, that he was unaware of any studies demonstrating the effectiveness of cameras and that there had been no comprehensive study of San Francisco's system. Yet, he continued to assert that cameras would deter crime.[81] Likewise, in Clovis, Police Captain Robert Keyes asserted that cameras contributed to a reduction in crime, despite the fact that "there's nothing other than anecdotal evidence to support that."[82] The ACLU survey found that no California jurisdiction with video surveillance cameras has conducted a comprehensive evaluation of their effectiveness.

As comprehensive studies strongly suggest cameras do not deter crime, the rationale of deterrence falls short of justifying either the cameras' expense or their intrusion into privacy.

FAILURE TO MEET EXPECTATIONS IN SOLVING VIOLENT CRIMES

Another justification for video surveillance is that its purported ability to capture evidence of criminal activity could potentially increase the success of criminal prosecutions. In London, the role of CCTV cameras in identifying the men involved in the 2005 terrorist attacks has been highly publicized.

Cameras undoubtedly capture some evidence of criminal activity, but in the limited studies available, evidence suggests that the impact of video footage on prosecutions may not be as significant as policy-makers expect.

First, some evidence suggests that cameras make little difference in the number of crimes actually solved. The Glasgow study cited above, for example, found that "the cameras appeared to have little effect on the clearance 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 percent. Once these figures were adjusted for general trends, however, the research analysts concluded that the clear-up rate fell from 64 to 60 percent."[83]

Second, while some crimes are certainly captured on film, some law enforcement agencies appear to overestimate the degree to which the footage helps law enforcement actually convict criminals. In Maryland, for example, Margaret Burns, 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."[84] According to a study by the Maryland state attorney's office, of the nearly 2,000 arrests made on the

basis of video camera footage, the vast majority concluded in an outright dismissal or a conviction for minor crimes. The office is now questioning the large amount of taxpayer money spent on the program. "Do these prosecutorial results support millions of dollars in tax expenditures? There will have to be a public debate about this," Burns said.[85]

In Cincinnati, Ohio, police also found cameras to be ineffective. A University of Cincinnati study found that the city's program, which began in 1998, merely shifted crime beyond the view of the cameras. 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."[86]

SPENDING ON CAMERAS: A TRADEOFF WITH MORE EFFECTIVE PROGRAMS

Video surveillance costs more than the cameras alone: The dollars used to buy the system are not spent in a vacuum. Public safety budgets are stretched very thin, especially in many urban areas, so money dedicated to video surveillance often comes at the expense of potentially more effective measures, such as lighting, community policing initiatives, and increased foot patrols.

Compare the lack of evidence of video surveillance's ability to reduce crime with the remarkable results that improved lighting produces. A survey commissioned by the British Home Office looked at 13 lighting studies in Great Britain and the United States and evaluated the cumulative impact. The study found a 20 percent average decrease in crime, with reductions in every area of criminal activity including violent crime. In fact, 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 individuals 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.[87]

Intensive foot patrols have shown similar results—reductions in crime, including violent crime, of 15 to 20 percent.[88] These findings suggest that from a law enforcement and public safety perspective alone, the dedication of scarce resources to video surveillance systems may not only be an inefficient and ineffective use of funds, it may actually be counterproductive.

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.'"

VIDEO SURVEILLANCE IN SAN FRANCISCO: EXPANSION WITHOUT STUDY OF ALTERNATIVES

At the direction of Mayor Gavin Newsom, San Francisco in June 2005 embarked on a 90-day pilot program by placing two video surveillance cameras on street corners outside a public housing project in the Western Addition neighborhood.[89] In October of that year, despite the lack of a comprehensive analysis of the effects of the program and with little public input, the mayor's office declared the program a success and expanded it by six additional cameras.[90] By March 2006 the program had grown to 33 cameras, all without meaningful evaluation or public debate.[91]

The San Francisco Board of Supervisors in May 2006, concerned about the expansion of the program without any formalized public process, passed a city ordinance establishing a process for determining camera placement. The ordinance mandated that before a camera could be placed, notice must be given to the surrounding community, and the police commission must find that the cameras' potential for deterrence would outweigh community concerns about the cameras and their use.[92]

The San Francisco Police Commission on January 17, 2007 held a hearing on the proposed placement of an additional 25 cameras at eight different locations throughout the city. At the hearing, commissioners heard testimony from numerous members of the public on both sides of the issue. More notable, however, was testimony from Allen Nance, Director of the Mayor's Office of Criminal Justice, who was promoting the cameras.

Nance admitted that his office had not conducted a comprehensive analysis of the existing cameras. The ACLU noted that the city had not even collected the data necessary to evaluate whether the cameras had actually prevented crime or had simply driven it elsewhere. Indeed, as the ACLU also noted at the hearing, the only data the city provided in response to ACLU requests for records of the city's evaluation showed that at more than half of the existing camera sites, crime actually *increased*.[93] Furthermore, the Samuelson Law, Technology and Public Policy Clinic at Boalt Hall School of Law, UC Berkeley, presented several studies indicating that cameras are ineffective in reducing crime. Meanwhile, Nance could not provide any evidence supporting his contention that they deter crime.[94]

Equally troubling was the failure of the Mayor's Office of Criminal Justice to consider alternatives. Referring to studies that have demonstrated that improved lighting significantly reduces crime, one commissioner asked Nance how much lighting could be purchased for the cost of the cameras; Nance could not answer. Though he was certain that his office would be requesting additional funds for even more cameras, he was not certain whether it would request more funding for lighting.[95]

The police commission approved the installation of additional cameras, but required the city to evaluate their effectiveness within six months.[96] To be effective, however, any future evaluation or budgeting for video surveillance must include a thorough analysis of whether crime has actually been prevented rather than just displaced, and alternatives and monetary tradeoffs must also be properly addressed.

PART III

PUBLIC RECORDS SURVEY
AND FINDINGS

The ACLU conducted surveys of cities throughout California to determine the extent of existing video surveillance systems, sending Public Records Act requests to a total of 131 jurisdictions statewide, including a diverse sample of agencies (in size, location, etc.) as well as cities already known to use cameras.

We specifically asked about public use of video surveillance cameras, excluding uses in city buildings such as the police department, intersections with red-light cameras, and police cars. We also asked about the types of camera systems that were being considered or had already been deployed.[97]

We received responses from 119 cities, nearly a third of which use or are in the process of considering some form of public video surveillance.

Our survey shows that the use of surveillance cameras is increasing rapidly and without regulation or evaluation of their effectiveness.

RISING NUMBER OF SURVEILLANCE CAMERAS

Eighteen jurisdictions reported having surveillance cameras on public streets. Some of these programs are relatively small, with just a few cameras currently in use. However, others are far broader, and several programs are being rapidly expanded. For example, Pittsburg recently purchased 13 cameras for use at various intersections and plans to add 32 more.[98] San Francisco, whose program started with two cameras in July 2005, now has 58 and plans to apply for Department of Homeland Security grants for more cameras in the coming years.[99] Santa Monica has a comprehensive system to provide nearly 100 percent visibility to police in the city's Third Street Promenade area, an outdoor public mall.[100] The largest recent expansion was in Fresno, where the city council approved $1.2 million for 73 cameras.[101]

Most of the surveillance camera systems in California were installed in the last few years. Seven of the 10 most extensive systems in Northern and Central California were installed in the last four years. Several of those cities and others throughout the state relied in part on Department of Homeland Security funding to establish their programs. The grants ranged from large awards, such as the $407,000 the city of Fresno received, to smaller grants to places like El Cajon.[102]

MEANWHILE, LITTLE OR NO REGULATION

Standing alone, the increased use of cameras is disturbing from a civil liberties perspective. On top of that, most of the programs are operating without any meaningful regulation. Only eleven of the 37 departments provided any written policies specifically addressing video surveillance. Clovis, for example, which has 35 cameras, had no policies governing their use (the city was reportedly in the process of drafting them).[103] Other cities, including Pittsburg (with 13 cameras) and Redding (with 35 cameras), lacked policies also.[104]

Even where policies exist, they are inadequate and often not legally enforceable. In Fresno, the new camera policy purports to prohibit the cameras' use for racial profiling. The camera policy, however, still allows the use of race as a factor in determining whom 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.[105]

Palm Springs has a wireless CCTV system monitoring the downtown commercial business district 24 hours a day, seven days a week. According to the Department's policy, "[t]he purpose of

Most of the video surveillance programs surveyed are operating without any meaningful regulation.

the CCTV cameras is to capture day-to-day criminal activity and to assist in response to crimes in progress." But while the policy prohibits "ongoing surveillance of specific individuals or groups" without a warrant, it does not bar "suspicionless" monitoring of speech activities, nor does it set guidelines that bar the use of race or gender as a factor in choosing subjects.[106]

In San Francisco, the surveillance program grew from two to 33 cameras without any binding regulations: Members of the mayor's staff and city organizations, such as the Emergency Services Department, promulgated policies, but these policies did not vest community members with any rights to seek redress for violations and were also easily changed. For example, camera footage originally was to be erased after 72 hours (three days), but the city changed that time span to seven days.[107] It was not until June 2006, almost a full year after the first cameras were installed, that the board of supervisors passed an ordinance providing for some legally enforceable regulations on public *processes* and the use of the cameras.[108]

ACTIVE MONITORING OF FOOTAGE

The lack of regulation of video surveillance is especially troubling because in 18 California jurisdictions police actively monitor the cameras, a situation that evidence from the British studies (see Section II) shows to be ripe for abuse.

NO ANALYSIS OF EFFECTIVENESS OR ALTERNATIVES

Finally, as local jurisdictions quickly expand the use of video surveillance, they are making little effort to evaluate its effectiveness. Several jurisdictions in our survey collected general crime statistics, but not a single one conducted a comprehensive analysis of the effectiveness of cameras or their relative benefits compared with other programs.

THERE IS A BETTER WAY: OAKLAND REJECTS VIDEO SURVEILLANCE TWICE

While many California cities rush to roll out video surveillance programs, one city considered and rejected them—twice. The Oakland city council, in both 1997 and 1999, rejected proposals to spend between $500,000 and $1 million on a video surveillance system.[109]

Council members fully evaluated both privacy concerns and evidence of the systems' effectiveness. Council member Henry Chang, an immigrant from China, reflected on his decision to come to the United States, saying, "We came because we don't want to be watched by Big Brother all the time."[110] Council member Nancy Nadel rejected the monetary tradeoffs, arguing that "it made me feel physical pain—the idea that we would spend public dollars on cameras before spending money to fight illiteracy."[111]

Council member Ignacio De La Fuente cast the deciding vote, citing a lack of evidence that cameras are effective in reducing crime and concluding that the program was not "worth the risk of violating people's privacy rights."[112]

Then-Mayor Jerry Brown concurred, saying that "reducing crime is something the community and police must work on together. Installing a few or a few dozen surveillance cameras will not make us safe. It should also not be forgotten that the intrusive powers of the state are growing with each passing decade."[113]

While the city has rejected a broad city-run camera system, it has allowed some public money to be used to fund cameras for businesses in public-private partnerships.[114]

PART IV

RECOMMENDATIONS AND CONCLUSION

Public video surveillance systems threaten privacy and, especially in combination with other technologies, have a real potential to radically change the relationship between the public and the government. Despite that risk, cities and agencies throughout California are increasingly deploying surveillance camera systems with little public debate or consideration of potential consequences. This is a serious mistake.

Video surveillance may be an appropriate technology to deploy in limited settings, such as in an airport or a police department. However, general monitoring of public space by the government is inappropriate in a free society. Existing and proposed video surveillance programs represent a disturbing trend. Even initially small programs that seem relatively benign have the potential to expand rapidly into larger ones.

To shift course and protect civil liberties, the California ACLU affiliates make the following recommendations:

RECOMMENDATION 1: Cease deploying surveillance cameras.

Reducing crime and apprehending criminals are worthy goals, but the evidence suggests that video cameras are generally ineffective in achieving them. Given surveillance cameras' limited usefulness and the potential threat they pose to civil liberties, the ACLU recommends that local governments stop deploying them.

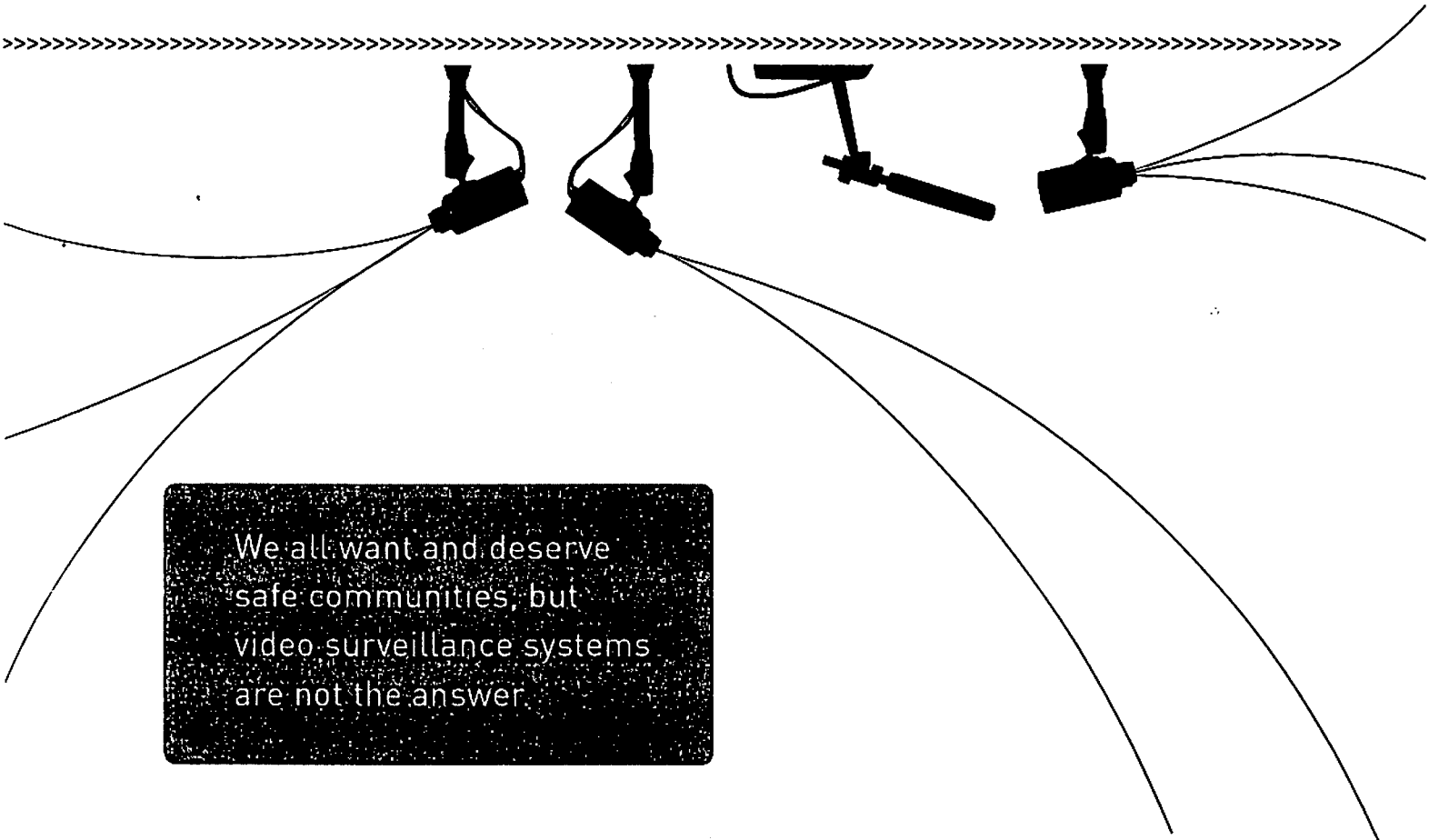
For cities considering cameras:

RECOMMENDATION 2: Evaluate other alternatives.

The ACLU recommends that local governments fully evaluate other crime reduction measures before spending limited public safety dollars on video surveillance systems.

RECOMMENDATION 3: Fully assess any proposed system's effectiveness and impact and establish a process for open public debate.

No city should deploy a technology without fully debating and considering its impact on members of the community. The ACLU recommends that any proposed video surveillance program be subjected to intense public scrutiny, and that the city conduct a full assessment of the system's effectiveness and impact on privacy and free speech before proceeding with the installation of cameras.



For cities with cameras already in place:

RECOMMENDATION 4: (Re)evaluate the system's effectiveness and its impact on privacy and hold public hearings.
The ACLU recommends that any city with a video surveillance system already in place conduct a comprehensive (re) evaluation of the system's effectiveness and impact on privacy. The city should make public the results of the evaluation and hold public hearings on the future of surveillance programs and possible alternative crime reduction measures. In the absence of evidence demonstrating measured effects on crime, consideration of alternatives, and full privacy and free speech assessments, camera systems should be removed.

Particularly at this time, when agencies at the federal, state, and local levels have monitored innocent Californians engaging in protected expressive activity, policy-makers and individual citizens must think critically about the deployment of even a single camera.[115] Once money is invested in a program, public agencies become much more willing to spend additional funds on expansion, rather than critically evaluate programs and consider alternatives.

We all want and deserve safe communities, but video surveillance systems are not the answer. Rather than investing money in invasive systems with marginal effectiveness, local governments must look at programs with proven results and that protect Californians' constitutional rights.

ENDNOTES

1 Several surveillance systems that were established in an effort to reduce crime in the 1970s and 1980s in cities such as Detroit, Atlantic City, and Charleston were ultimately abandoned because of cost and ineffectiveness. "Why Legal Action Against the City of New York Should Be Taken for its Installation of Surveillance Cameras in Public Places." March, 2001. Surveillance Camera Players, accessed on July 26, 2007 on the World Wide Web at http://www.notbored.org/to-the-lawyers.html; see also Marcus Nieto, "Public Video Surveillance: Is It An Effective Crime Prevention Tool?," California Research Bureau, June 1997, available at http://www.library.ca.gov/CRB/97/05/.

2 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.

3 See e.g. Cisco Systems. "City of Brentwood." 2004. Accessed via the World Wide Web on January 26, 2007 at http://www.cisco.com/web/strategy/docs/gov/local_Brentwood.pdf.

4 Robert Selna, "Oakland Pulls Plug On Crime Cam Plan," *San Francisco Examiner*, 1999.

5 Moore, *supra* note 3; Jessica Bennett, "Big Brother's Big Business," Newsweek, Mar. 15, 2006.

6 Fran Spielman, "Daley: By 1016, Cameras on 'Almost Every Corner,'" *Chicago Sun Times*, Oct. 12, 2006.

7 Linda Bryant, "Exploring the Potential Legal Issues that May Result from Using a Built-In Microphone in CCTV Applications," Video Surveillance Guide, Feb. 15, 2007, http://www.video-surveillance-guide.com/microphone-cctv.htm (discussing the legal implications of consumer CCTV cameras with built-in microphones); Brickhouse Security, "Hidden Spy Cameras Designed to Protect Your Family & Property," http://www.brickhousesecurity.com/covert-hidden-spy-cameras.html (describing camera systems offered for sale, including built-in audio recording) (last visited Apr. 11, 2007).

8 Demian Bulwa, "Future Fuzzy for Government Use of Public Surveillance Cameras," *San Francisco Chronicle*, July 23, 2006, at A-1, 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.

9 "Who Watches The Watchers In Surveillance Society?," *Reuters*, Feb. 4, 2007 at http://www.informationweek.com/shared/printableArticle.jhtml?articleID=197003126; see also Object Video website at http://www.objectvideo.com/ (descriptions of products and uses).

10 Tom Abate, "Surveillance Via Software Helps SFO," *San Francisco Chronicle*, July 24, 2006, at C-1, available at http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2006/07/24/BUGEHK1UA21.DTL.

11 *Id.*

12 *Id.*

13 Jeremy Bentham, *4 The Works of Jeremy Bentham*, 37-172 (John Bowring ed., 1962) (1838-1843).

14 Michael Foucault, *Discipline and Punish*, 195-229 (Alan Sheridan, trans., Vintage Books 2d ed. 1995) (1978).

15 George Orwell, *Nineteen Eighty-Four*, 205 (Sygnet Classics 1977) (1949).

16 "LAPD Experimenting with Facial-Recognition Software," *San Diego Union Tribune*, Dec. 26, 2004, available at http://www.signonsandiego.com/uniontrib/20041226/news_1n26lapd.html.

17 Bill Christensen, "Stealthy Iris Scanner in the Works," *LiveScience*, Feb. 6, 2007, at http://www.livescience.com/scienceofiction/070206_technovelgy.html.

18 This combination has not happened yet, but it is not far off. As RFID readers become more and more sophisticated the ability to combine video surveillance and RFID readers will increase.

19 For more information about the use of RFID technology in identification documents, please see "The Use of RFID for Human Identification: A Draft Report from The Department of Homeland Security Emerging Applications and Technology Subcommittee to the Full Data Privacy and Integrity Advisory Committee," (May 2006), available at http://www.dhs.gov/xlibrary/assets/privacy/priva-

cy_advcom_rpt_rfid_draft.pdf [hereinafter DHS Subcommittee Report]; Government Accountability Office, "Informaton [sic] Security: Radio Frequency Identification Technology in the Federal Government," (May 2005), available at http://www.gao.gov/new.items/d05551.pdf; ACLU of Northern California, "RFID in Identification Documents," at ACLU of Northern California, "Don't Chip Our Rights Away!," at http://www.aclunc.org/issues/technology/dont_chip_our_rights_away!.shtml (last visited Apr. 11, 2007); The Electronic Frontier Foundation (EFF), Radio Frequency Identification (RFID), at http://www.eff.org/Privacy/RFID/ (last visited Apr. 11, 2007); The Electronic Privacy Information Clearinghouse (EPIC), Radio Frequency Identification (RFID) Systems, at http://www.epic.org/privacy/rfid/ (last visited Apr. 11, 2007).

20 DHS Subcommittee Report, *supra* note 19.

21 "Rights 'Chipped' Away: RFID in Identification Documents," forthcoming Fall 2007, Stanford Technology Law Review. Draft available at http://aclunc.org/issues/technology/dont_chip_our_rights_away!.shtml.

22 American Civil Liberties Union, Real Nightmare.org, www.realnightmare.org (the ACLU's Web site on the Real ID Act) (last visited Apr. 11, 2007); EPIC, National ID Cards and Real ID Act (EPIC's Web site on the Real ID Act) (last visited Apr. 11, 2007).

23 Real ID permits but does not require, Homeland Security to mandate that biometric identifiers such as fingerprints, retinal scans, or DNA samples be included. Declan McCullagh. "State Officials Oppose Repealing Real ID Act," *CNET News.com*, Feb. 8, 2007 http://news.zdnet.com/2100-1009_22-6157813.html.

24 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..." EPIC, Choicepoint, http://www.epic.org/privacy/choicepoint/ for more information (EPIC's webpage on Choicepoint) (last visited Apr. 11, 2007).

25 Christopher Slobogin, "Public Privacy: Camera Surveillance of Public Places and The Right to Anonymity," 72 Miss. LJ 213, 233 (2002) (citing Richard Wasserstrom,"Privacy: Some Arguments and Assumptions," in Philosophical Dimensions of Privacy, 325-26 (Ferdinand David Schoeman, ed., Cambridge Univ. Press 1984).

26 Slobogin, *supra* note 24 at 244 (citing Nicholas C. Burbules, "Privacy, Surveillance, and Classroom Communication on the Internet", Access, vol. 16, 42-50 (1997) available at http://faculty.ed.uiuc.edu/burbules/papers/privacy.html.

27 *Chicago v. Morales*, 527 U.S. 41, 53-54 (1999).

28 J. Rosen, "Being Watched: A Cautionary Tale for a New Age of Surveillance," *New York Times*, Oct. 7, 2001. Accessed via World Wide Web at https://www.nytimes.com/29001/10/07/magazine/07SURVEILLANCE.html.

29 Ironically, while cameras may affect people engaging in innocent behavior, they have very little impact on criminal behavior. Because some crime is irrational, and rational criminals find ways around cameras, studies show that video surveillance does not significantly reduce crime, see *infra* Section II.

30 This is particularly true when video surveillance is combined with facial recognition and RFID technology.

31 *Buckley v. Am. Constitution Law Found.*, 525 U.S. 182 (1999) (striking down Colorado's requirement for petition solicitors to wear an identification badge because it "discourages participation in the petition circulation process by forcing name identification without sufficient cause."); *McIntyre v. Ohio Elections Commission*, 514 U.S. 334 (1995) (striking down an Ohio law prohibiting the distribution of anonymous campaign literature and taking note of "a respected tradition of anonymity in the advocacy of a political cause."); *Lamont v. Postmaster General*, 381 U.S. 301 (1965) (striking down government measure that required individuals to notify the post

office of interest in certain political materials before receiving them in the mail); *Talley v. California*, 362 U.S. 60 (1960) (striking down a ban on anonymous handbills, noting that "(p)ersecuted groups and sects from time to time throughout history have been able to criticize oppressive practices and laws...anonymously.")

32 *NAACP v. Alabama*, 357 U.S. 449 (1958) (forbidding the state of Alabama from compelling the NAACP to disclose its membership lists).

33 See also *Presbyterian Church (U.S.A.) v. United States*, 870 F.2d 518 (9th Cir. 1989) (church suffered harm of diminished membership as a result of surveillance); Olagues v. Russoniello, 797 F.2d 1511 (9th Cir. 1986) (plaintiffs were targets of surveillance).

34 *McIntyre*, 514 U.S. at 341-42.

35 *Katz v. United States*, 389 U.S. 347, 351 (1967) (reversing Court's ruling in Olmstead v. United States, 277 U.S. 438 (1928) and holding that wiretap of public telephone violated Fourth Amendment). There is also a line of cases in which the courts have concluded that certain factual situations do not warrant a reasonable expectation of privacy. See, e.g., *United States v. Knotts*, 460 U.S. 276, 281 (1983) (tracking car's movements with an electronic beeper did not violate the Fourth Amendment because " [a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.")

36 *Katz*, 389 U.S. 347.

37 Hammond, Susan, "Web-Watch: Emergency Access to Security Web-Cam Systems," Corona Police Department and Corona Chamber of Commerce. ACLU received PRA response on Dec. 19, 2006.

38 *Id.*

39 "Oakland: Oakland Installs Video Surveillance Cameras," *NBC 11*, posted Nov. 15, 2005. Accessed via the World Wide Web on May 30, 2007 at http://www.officer.com/article/article.jsp?id=26728&siteSection=1. Brentwood: Clare Computer Solutions. "Case History: City of Brentwood," Sept. 2004. Accessed via the World Wide Web on Jan. 26, 2007 at www.clarecomputer.com/CityofBrentwood.pdf.

40 *White v. Davis* (1975) 13 Cal.3d 757, 774 (quoting ballot argument in support of the privacy amendment).

41 *Id.*

42 *Terry v. Ohio*, 392 U.S. 1, 27 (1968) (holding that pat-downs require reasonable suspicion).

43 *Katz*, 389 U.S. at 351.

44 *Talley v. California*, 362 U.S. 60 (1960); Schneider v. State of New Jersey, 308 U.S. 147, 162 (1939); see also Jamison v. Texas, 318 U.S. 413 (1943) (declaring unconstitutional a city's ordinance that prohibited the distribution of leaflets and expressly rejecting the city's argument of an absolute right to control speech on public property).

45 *Delaware v. Prouse*, 440 U.S. 648, 663 (1979) (citation omitted).

46 *Katz*, 389 U.S. at 351 ("[W]hat a person seeks to keep private, even in an area accessible to the public, may be constitutionally protected").

47 *Hague v. CIO*, 307 U.S. 496, 515 (1939) (Roberts, J., concurring).

48 *Buckley v. Am. Constitution Law Found.*, 525 U.S. 182 (1999) (striking down Colorado's requirement for petition solicitors to wear an identification badge because "discourages participation in the petition circulation process by forcing name identification without sufficient cause."); *McIntyre v. Ohio Elections Commission*, 514 U.S. 334 (1995) (striking down an Ohio law prohibiting the distribution of anonymous campaign literature and taking note of "a respected tradition of anonymity in the advocacy of a political cause."); *Lamont v. Postmaster General*, 381 U.S. 301 (1965) (striking down government measure that requires individual to notify the post office of interest in certain political materials before receiving them in the mail); *Talley*, 362 U.S. 60 (striking down a ban on anonymous handbills, noting that "(p)ersecuted groups and sects from time to time throughout history have been able to criticize oppressive practices and laws...anonymously").

49 Marc Delehanty, "WifiLlinks Vulnerable Even with Encryption," *Personal Computer World*, July 27, 2006, http://www.crn.com.au/story.aspx?CIID=57402.

50 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. Webopedia, Definition of 802.11, http://www.webopedia.com/TERM/8/802_11.html (last visited Apr. 11, 2007); Dan Verton, "Flaws in Wireless Security Detailed: Cracked Algorithm, Holes in

802.11 Spec Mean Companies Need More Authentication," *Computer-World*, July 16, 2001, http://www.computerworld.com/securitytopics/security/story/0,10801,62220,00.html. Examples of research detailing 802.11 security vulnerabilities available at William A. Arbaugh, Wireless Research: 802.11 Security Vulnerabilities, http://www.cs.umd.edu/~waa/wireless.html (last visited Apr. 11, 2007).

51 Dibya Sarkar, "City of Ripon Goes Wireless," *FCW.com* (*Federal Computer Week*), June 20, 2005, http://www.fcw.com/article89302-06-20-05-Print.

52 See also "The Earthlink/Google Proposal for the City and County of San Francisco," Feb. 2006, http://www.sfgov.org/site/uploadedfiles/dtis/tech_connect/EarthLink_San-Francisco_RFP_2005-19_PUBLIC.pdf at 24.

53 "300 Municipal WiFi Systems in the U.S.," *Daily Wireless.Org*, Jan. 2, 2006, http://www.dailywireless.org/2007/01/02/300-municipal-WiFi-systems-in-us/ (citing muni-wireless.com). See, e.g., "Tropos Networks, Saving Lives with Tropos MetroMesh: City of New Orleans, Louisiana, A Tropos Networks Case Study" (June 2005) http://www.tropos.com/pdf/new_orleans_casestudy.pdf.

54 Government Code section 6254(f) contains an exception for certain law enforcement information.

55 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.

56 *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).

57 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).

58 http://www.ktvu.com/news/4398749/detail.html (last visited Oct. 26, 2006).

59 Thomas J. Nestel III, "Using Surveillance Camera Systems to Monitor Public Domains: Can Abuse Be Prevented?" master's thesis, Naval Postgraduate School, Monterey, Calif., Mar. 2006.

60 Clare Computer Solutions. "Case History: City of Brentwood.," Sept. 2004. Accessed via the World Wide Web on January 26, 2007 at www.clarecomputer.com/CityofBrentwood.pdf.

61 Black, J. "Smile, You're On Surveillance Camera," *Business Week*, Oct. 17, 2003. Accessed via the World Wide Web on January 3, 2007 at http://www.businessweek.com/bwdaily/dnflash/oct2003/nf20031017_2392_db025.htm?chan=search.

62 "Word On The Street...They're Listening," *The Sunday Times*, Nov. 26, 2006. Accessed via the World Wide Web on Jan. 3, 2007 at http://www.timesonline.co.uk/tol/news/uk/article650166.ece.

63 J. Bennetto, "Big Brother Britain 2006: We Are Waking Up To A Surveillance Society All Around Us," *Independent*, Nov. 2, 2006. Accessed via the World Wide Web on Jan. 3, 2007 at http://www.commondreams.org/headlines06/1102-07.htm.

64 *Id.*

65 D. Neawedde, "Surveillance Cams That Talk! Not Quite," Ministry of Technology, Sept. 18, 2006. Accessed via the World Wide Web on January 3, 2007 at http://www.ministryoftech.com/index.php?s=surveillance+cams+talk.

66 *Id.*

67 M. Rice-Oxley, "Big Brother In Britain: Does More Surveillance Work?" *The Christian Science Monitor*, Feb. 6, 2004. Accessed via the World Wide Web on Jan. 3, 2007 at http://www.csmonitor.com/2004/0206/p07s02-woeu.html.

68 "Police Chief's 'Orwellian' Fears," *BBC News*, May 20, 2007, available online at http://news.bbc.co.uk/1/hi/uk/6673579.stm.

69 M. Norris, "Video Cams Help Cities Deter Crime," Nov. 3, 2006. Accessed via the World Wide Web on Jan. 26, 2007 at www.oakleypress.com.

70 Jim Zulim, Correspondence between City of Clovis Police Department and City of Clovis Department of Finance, July 28, 2003.

71 Correspondence between Chief Bradley Ramos & Capt. Mark Miller. Investigative Services Bureau Coordinator; Indio Police Department. February 1, 2007.

72 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).

73 "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").

74 Brandon C. Welsh and David P. Farrington, "Crime Prevention Effects of Closed Circuit Television: A Systematic Review," Home Office Research Study 252, Aug. 2002, at p. iv.

75 Martin Gill and Angela Spriggs, "Assessing the Impact of CCTV," Home Office Research Study 292, Feb. 2005, at p. 58.

76 Glasgow Study, *supra*, note 73.

77 Gill and Spriggs, *supra*, note 73.

78 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 management. com/library/000236.html; Rosemary Erickson, "Armed Robbers and Their Crimes," Chapter 4, 1996, available at https://www.securitymanagement. com/library/000235.html.

79 *Id.*

80 Gill and Loveday, "What Do Offenders Think About CCTV," 2003, p. 24.

81 Allen Nance, "Police Commission Hearing," Jan. 17, 2007. Accessed via the World Wide Web at http://sanfrancisco.granicus.com/ViewPublisher.php?view_id=21

82 D. Bulwa, "Future Fuzzy For Government Use Of Public Surveillance Camera—Still, Some Bay Area Cities Hope To Follow Clovis' Lead," *San Francisco Chronicle*. July 23, 2006. Accessed via the World Wide Web on Jan. 24, 2007 at http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2006/07/23/MNGC0K45G21.DTL&hw=future+fuzzy&sn=001&sc=1000.

83 Glasgow Study, *supra*, note 73.

84 Matthew Cella, "Statistics Show Cameras Limited in Decreasing Violent Crime," *Washington Times*, Aug. 14, 2006.

85 Luke Broadwater, "Prosecutors: Stats Show Blue Light Cameras not Getting Results," *San Francisco Examiner*, Jan. 22, 2007.

86 Christina Ramirez and Lisa Hoffman, "Video Becomes a Crime Fighting Tool," *Capitol Hill Blue*, June 23, 2006.

87 David P. Farrington and Brandon C. Welsh, "Effects of Improved Street Lighting on Crime: A Systematic Review," Home Office Research Study 251, Aug. 2002, p. 42.

88 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 R. crime).

89 R. Gordon, "Cameras To Fight Crime Round-the-Clock Surveillance Outside Housing Project," *San Francisco Chronicle*, July 30, 2006. Accessed via the World Wide Web on Jan. 22, 2007 at http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2005/07/30/BAG7HE07481.DTL&hw=Cameras+to+fight+crime&sn=003&sc=582

90 R. Gordon, "Mayor Wants Wider Surveillance Program," *San Francisco Chronicle*, Oct. 12, 2006. Accessed via the World Wide Web on Jan. 22, 2007 at http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2005/10/12/BABADIGEST4.DTL&hw=Mayor+wants+wider&sn=001&sc=1000

91 D. Bulwa, "Police Commission Decides On Plan For More Street Cameras," *San Francisco Chronicle*, Jan. 17, 2007. Accessed via the World Wide Web at. http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2007/01/17/BAGHNNKDKI13.DTL&hw=Police+Cameras+2005&sn=002&sc=1000

92 San Francisco Municipal Code Chapter 19, Community Safety Camera Ordinance.

93 "Crime Goes Up in More Than Half of SF Location," available at http://www.aclunc.org/issues/technology/say_no_to_video_surveillance.shtml

94 Allen Nance, "Police Commission Hearing," Jan. 17, 2007. Accessed via the World Wide Web at http://sanfrancisco.granicus.com/ViewPublisher.php?view_id=21

95 *Id.*

96 *Id.*

97 Other information requested included crime statistics before and after camera deployment and information about funding sources.

98 R. Ziegler, "Request for Public Records Related to Video Surveillance Cameras," Sept. 7, 2006. Written Correspondence from Pittsburg City Attorney to ACLUNC.

99 Mayor's Office of Criminal Justice. "Community Safety Cameras--Frequently Asked Questions," Jan. 2, 2007. Accessed via the World Wide Web on February 14, 2007 at http://www.sfgov.org/site/uploadedfiles/mocj/Community%20Safety%20Camera%20Frequently%20Asked%20Questions(1).pdf; Police Commission Hearing January 17, 1007, *supra*, note 94.

100 City of Santa Monica. "Request for Proposal: Public Video Security System," P.2-3. (RFP undated, but requests were due by 10.3.05); Eric Uller. Telephone conversation between Peter Bibring and Eric Uller, Santa Monica Police Department, March 19, 2007.

101 Deirdre K. Mulligan and David E. Snyder, "It's Not Too Late to Debate Video Surveillance," *Fresno Bee*, July 19, 2006.

102 Mark Arner and Anne Kueger, "Mobile Tower to Watch Over Mall," *San Diego Union Tribune*, Oct. 21, 2006.

103 D. Bulwa, "Future Fuzzy For Government Use Of Public Surveillance Cameras—Still, Some Bay Area Cities Hope To Follow Clovis' Lead," *San Francisco Chronicle*. July 23, 2006. Accessed via the World Wide Web on January 24, 2007 at http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2006/07/23/MNGC0K45G21.DTL&hw=future+fuzzy&sn=001&sc=1000.

104 City of Pittsburg. Ziegler, R., "Request for Public Records Related to Video Surveillance Cameras," Sept. 7, 2006, Meyers, Nave, Riback, Silver & Wilson; City of Redding: DeWalt, Barry, "Public Record Act Request Dated June 26, 2006," Aug. 3, 2006, Office of the City Attorney.

105 "Video Policing Project Policy and Guidelines Manual," July 2006, Fresno Police Department.

106 The Office of the Chief of Police. "Downtown Video Surveillance Camera Policy." General Order 2002-05. Palm Springs Police Department. April 22, 2002.

107 San Francisco Emergency Communications Department. Standard Operating Procedures, "Community Safety Camera Digital Recordings," effective July 27, 2005, revised Dec. 10, 2005.

108 San Francisco Municipal Code Chapter 19, *supra*, note 92.

109 Police Services Agency, "Public Safety Committee: Video Surveillance Cameras," City of Oakland Agenda Report, Sept. 16, 1997; B. Payton, "Cheers for City 'Council's rejection of surveillance cameras," *Oakland Tribune*, East Bay Hills, June 17, 1999.

110 K. Kirkwood, "Oakland To Debate Camera Tracking," *Oakland Tribune*, June 2, 1999.

111 B. Payton, *supra*, note 109.

112 B. Payton, *supra*, note 109.

113 Robert Selna, "Oakland Pulls Plug On Crime Cam Plan," June 16,1999, *San Francisco Examiner*.

114 Laura Ernde, "With Nod From City, Merchants Focus On Crime," *Oakland Tribune*, Feb. 4, 2005. Accessed via the World Wide Web at http://www.findarticles.com/p/articles/mi_qn4176/is_20050224/ai_n11844485.

115 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 Sept. 11, 2001).

Published August 2007

By the ACLU of Northern California

Find this report online at www.aclunc.org

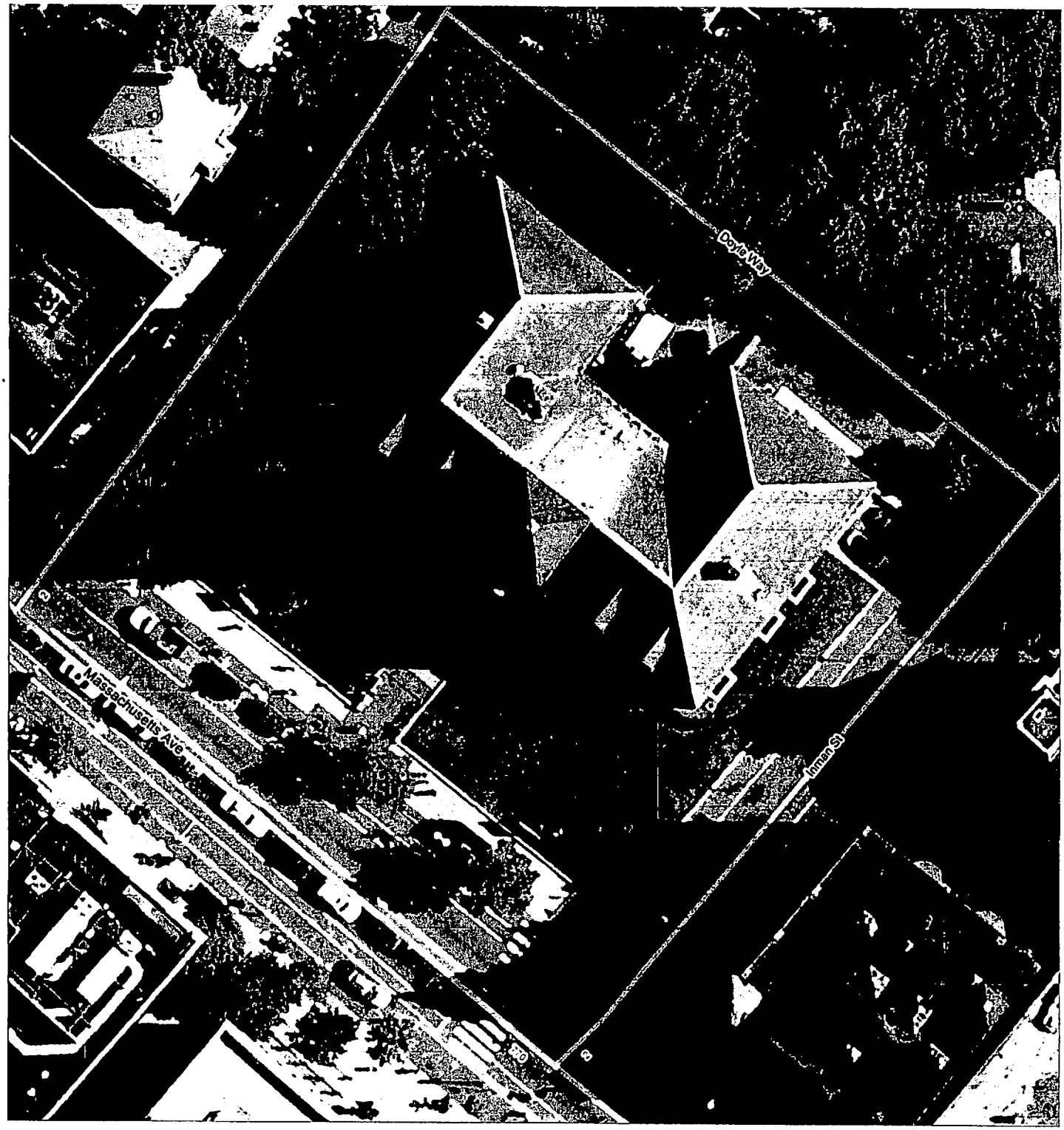
39 Drumm Street San Francisco California 94111
415 621 2493 WWW.ACLUNC.ORG

1616 Beverly Blvd. Los Angeles California 90026
213 977 9500 WWW.ACLU-SC.ORG

P.O. Box 87131 San Diego California 92138
619 232 2121 WWW.ACLUSANDIEGO.ORG

Google Maps

To see all the details that are visible on the screen, use the "Print" link next to the map.



E

I am John Moon, Professor Emeritus of History. I am the co-editor of a book on biological warfare published by Oxford University Press. Currently, I am under contract to Harvard University Press to write a book on the American biological warfare program.

Since I have spent many years studying and writing on the history weapons of mass destruction [WMD], let me address the argument that they would be useful in carrying out an evacuation. Against which weapon? Against chemical, biological, radiological and nuclear weapons? In the case of a nuclear attack, evacuation would be futile. Such a proposal merely echoes the escape fantasies indulged by policy makers during the Cold War. In the case of a radiological attack, the geographical area would be limited. It would be more sensible to evacuate affected residents from the stricken area to another

part of Greater Boston. In the case of a chemical attack, the effect would also limited to the area in which the attack was launched and to those struck by the agents. Non-persistent agents would be quickly dissipated; areas struck be persistent agents, like mustard, would of course, have to be put off limits and decontaminated. In the case of a biological attack, the symptoms attending the disease would probably not be detected until several days after the attack took place. And would they be properly and speedily diagnosed?

The exit scenario is based on a worst case event: a massive and sustained attack upon the city of Boston by an opponent armed with a formidable arsenal of

weapons of mass destruction. Terrorists can do a lot of localized damage. But they do not now enjoy the capability to inflict damage on the monumental scale that the Soviet Union was capable of inflicting.

An attempt to carry out a mass evacuation would create disruption, panic and confusion. If you consider the victims, they could be far better treated if they remained within the Greater Boston area, which enjoys such superb medical facilities, rather than moved outside its perimeter. The training of first responders in the management of a WMD attack, the development of vaccines and the placement of reliable detection devices which could identify biological agents in real time without yielding false

positives would represent far more effective means in dealing with the consequences of a WMD attack.

We recognize that certain strategic facilities (e.g. airports, military bases, sea ports, communications centers, etc.) need surveillance. But the exit routes through Brookline? Manipulating understandable fears regarding public safety, the outgoing administration has created a surveillance system, which is out of control and threatens to become more and more extensive. There is no such thing as total security. If we pursue that illusory goal, we will end up being neither secure nor free.

Thanking you for your consideration,

John Ellis van Courtland Moon

Professor of History Emeritus

11 Monmouth Court

Brookline, Massachusetts 02446

CITY COUNCIL

Policy Order Resolution

O-2
IN CITY COUNCIL

April 7, 2008

COUNCILLOR KELLEY
MAYOR SIMMONS
COUNCILLOR MAHER
COUNCILLOR DAVIS
COUNCILLOR DECKER
COUNCILLOR REEVES
COUNCILLOR SEIDEL
COUNCILLOR TOOMEY

WHEREAS: There have been concerns expressed about public safety at the newly renovated Russell Field athletic complex; and

WHEREAS: These concerns may be somewhat addressed through the installation of more extensive security cameras in that area; and

WHEREAS: The MBTA already has a system of security cameras connected to the area immediately around the Alewife T station; and

WHEREAS: Some people have privacy concerns about too many cameras monitoring their public activities; now therefore be it

ORDERED: That the City Manager be and hereby is requested to have Cambridge Police Department staff confer with relevant MBTA staff to determine the extent of area coverage by the MBTA cameras and to determine where additional security cameras could be most effectively deployed to improve public safety in this area; and be it further

ORDERED: That the City Manager be and hereby is requested to report back to the City Council on the feasibility of installing additional security cameras in this area to address public safety concerns; and be it further

ORDERED: That the City Manager be and hereby is requested to confer with the Police Commissioner, the Commissioner of Public Works and other relevant City and School Department staff to determine and implement appropriate short-term security measures for this area; and be it further

ORDERED: That the Civic Unity Committee be and hereby is requested to have a public hearing on security cameras within the next 45days with the intent of at least starting to develop some comprehensive guidance for the deployment of municipal security cameras.

In City Council April 7, 2008
Adopted by the affirmative vote of nine members.
Attest:- D. Margaret Drury, City Clerk

G

CIVIC UNITY STATEMENT

The proposal to set up surveillance cameras in our city is a fundamentally bad idea.

It would amount to yet another assault on our civil liberties. After suffering eight years of erosion of these rights by the Bush administration, we would be assenting to a further narrowing of our privileges.

In his inauguration speech Barack Obama said: "As for our common defense, we reject as false the choice between our safety and our ideals."

Placing these cameras in public vantage points would violate our privacy. We would be accepting the federal and state governments infringing on our freedom to walk city streets without our every move being recorded and preserved.

I feel special concern for the young people of our community. They are already in danger of growing up thinking it normal for America to be fortified on every front against supposed terrorists.

Among other things, they will take it for granted that most public buildings (fortunately not our city hall) and many private ones require you to empty your pockets and pass through electronic sensors before entering. And, if they know about it at all, they see as ordinary the MBTA having some 500 cameras to record riders entering subway stations and riding buses.

They will be unbelieving when those of us who lived longer tell them that America did not used to be like that. It will sound like fantasy when we tell them we were never exposed to announcements telling us to inform on others when they looked at all suspicious.

Until recent years we could walk into the state house and other public buildings without submitting to bothersome inspection. And, when walking downtown, we did not need to fear being photographed.

Young people will have trouble believing all this because our society has bought the need to sacrifice so much in the name of protection against terrorists. If only they were aware of our losses, perhaps they would join those of us who oppose further extensions of the fortress mentality.

The America we have known and loved stands in danger of being lost. Is the focus on security worth it?

About the widespread use of surveillance cameras in particular one must be skeptical. Experience shows how law-abiding citizens who engage in political protest or other activity not infrequently suffer repression or arrest. The example of what police did in Boston and New York during national party conventions should make us wary of cameras to record demonstrators' faces.

The ways in which the FBI has infringed upon the rights of people who have done nothing illegal should also serve to make us unwilling to have our citizens' images entered into data banks. War protestors and others can find themselves under suspicion for years when they have done nothing wrong.

We have inadequate information about how the data gathered by cameras would be used. Who will have access to the data? We do not know. Other unanswered questions remain and some of them will probably never be answered, all in the name of security.

I call upon the city council to turn down the offer of funds to establish surveillance cameras in our city.

Richard Griffin