INCLUDING MODEL LEGISLATION

GUIDELINES FOR PUBLIC VIDEO SURVEILLANCE




A GUIDE TO PROTECTING COMMUNITIES AND PRESERVING CIVIL LIBERTIES

THE CONSTITUTION PROJECT

GUIDELINES FOR PUBLIC VIDEO SURVEILLANCE

A GUIDE TO PROTECTING COMMUNITIES AND PRESERVING CIVIL LIBERTIES

A REPORT OF THE CONSTITUTION PROJECT'S
LIBERTY AND SECURITY COMMITTEE

For information about this report, or any other work of the Constitution Project, please visit our website at www.constitutionproject.org or e-mail us at info@constitutionproject.org.

CONSTITUTION PROJECT STAFF

Tara Beech
Program Assistant

Sharon Bradford Franklin
Senior Counsel

Joseph N. Onek
Senior Counsel

Katy Dyer
Communications Coordinator

I. Scott Messinger
Director of Management and Operations

Virginia E. Sloan
President and Founder

The Constitution Project
1025 Vermont Avenue, NW
Third Floor
Washington, DC 20005

(202) 580-6920 (tel)
(202) 580-6929 (fax)

info@constitutionproject.org
www.constitutionproject.org

TABLE OF CONTENTS

PREFACE

The Constitution Project is a bipartisan, nonprofit organization that seeks consensus on controversial legal and political issues through scholarship and advocacy. In the days following the September 11, 2001 terrorist attacks on the United States, the Constitution Project launched its Liberty and Security Initiative. Guided by an ideologically diverse committee of prominent Americans, the Initiative addresses a wide range of issues, including the tension between rapidly changing technology used to enhance security and constitutional values relating to personal liberty and privacy. The Initiative is committed to developing and advancing proposals to protect civil liberties even as our country works to make Americans safe.

While much attention has been paid to efforts on the federal level to enhance our safety in the aftermath of September 11th, state and local programs also directly affect the security and civil liberties of Americans. For many communities, the desire to implement video surveillance systems stems not from a reaction to September 11th, but from the desire for crime control. This report is designed to provide a set of practical guidelines for state and local officials who are contemplating installation of—or who have already installed—public video surveillance systems. Through these guidelines, the Constitution Project's Liberty and Security Initiative seeks to demonstrate that communities can choose to implement such security systems in ways that protect residents' privacy rights and civil liberties.

The Constitution Project sincerely thanks the law firm of Wilmer Cutler Pickering Hale and Dorr LLP for its invaluable work researching and drafting this report. In particular, we thank Marc Jonathan Blitz, now a Professor at the Oklahoma City University School of Law, who conducted the initial research and worked with the Initiative to craft recommendations to reconcile constitutional values with law enforcement and anti-terrorism goals; and Will T. DeVries, who shared with us his expertise in law and technology, as well as his skills in writing a practical report that will be informative to policymakers, the legal community, the media, and the public at large.

The Constitution Project also thanks the Samuelson Law, Technology & Public Policy Clinic at U.C. Berkeley's Boalt Hall School of Law, including its Director, Deirdre K. Mulligan, and students, Tara Wheatland, David C. Yang, and Peter Maybarduk, for their important research and drafting assistance. In particular, we thank the clinic members for their extensive work in drafting model legislation to codify the Constitution Project's guidelines. We hope that the model legislation—included at the end of this report—will enable state and local government officials to adopt these recommendations with ease.

Finally, we are grateful to the Public Welfare Foundation and the Community Foundation for their support of the Liberty and Security Initiative's work on the Constitution Project's *Guidelines for Public Video Surveillance.* We also thank the Open Society Institute, the Wallace Global Fund, and an anonymous donor for their support of the Constitution Project in all its work.

–Joseph N. Onek, Senior Counsel
–Sharon Bradford Franklin, Senior Counsel

Members of the Liberty and Security Initiative Endorsing the Constitution Project's *Guidelines for Public Video Surveillance**

Co-Chairs

David Cole—Professor of Law, Georgetown University Law Center

David Keene—Chairman, American Conservative Union

Members

Floyd Abrams, Esq.—Partner, Cahill Gordon & Reindel LLP

Dr. Azizah Y. al-Hibri—Professor, The T.C. Williams School of Law, University of Richmond; President, Karamah: Muslim Women Lawyers for Human Rights

The Honorable Bob Barr—former Member of Congress (R-GA); CEO, Liberty Strategies, LLC; 21st Century Liberties Chair for Freedom and Privacy at the American Conservative Union; Chairman of Patriots to Restore Checks and Balances; practicing attorney; Consultant on Privacy Matters for the ACLU

John J. Curtin, Jr.—Bingham McCutchen LLP; former President, American Bar Association

The Honorable Mickey Edwards—Director, Aspen Institute-Rodel Fellowships in Public Leadership; Lecturer, Woodrow Wilson School of Public and International Affairs, Princeton; former Member of Congress (R-OK); former Chairman, House of Representatives Republican Policy Committee

Dr. Morton H. Halperin—Director of U.S. Advocacy, Open Society Institute; Senior Vice President, Center for American Progress

David Lawrence, Jr.—President, Early Childhood Initiative Foundation; former Publisher, *Miami Herald* and *Detroit Free Press*

Stephen M. Lilienthal—Director, Center for Privacy and Technology Policy, Free Congress Foundation

Kate Martin—Director, Center for National Security Studies

John Podesta—President and CEO, Center for American Progress; White House Chief of Staff, Clinton Administration

The Honorable William S. Sessions—former Director, Federal Bureau of Investigation; former Chief Judge, United States District Court for the Western District of Texas

John Shore—Founder and President, noborg LLC; former Senior Advisor for Science and Technology to Senator Patrick Leahy

John F. Terzano—President, The Justice Project

John W. Whitehead—President, The Rutherford Institute

Roger Wilkins—Clarence J. Robinson Professor of History and American Culture, George Mason University

** Organizational information is listed for identification purposes only.*

EXECUTIVE SUMMARY

Courts, lawmakers, and legal scholars have grappled for decades with how best to regulate law enforcement use of video surveillance in light of the constitutional rights and values such surveillance implicates. To this point, most decision-makers have simply defaulted to those minimum protections established by existing constitutional jurisprudence and the practical limits of the technology. Constitutional law protects the home and other private spaces and, for the most part, video cameras were not capable of changing the anonymous nature of the public streets.

In recent years, however, technological advances and social changes have ushered in new and more pervasive forms of public video surveillance with the potential to upset the existing balance between law enforcement needs and constitutional rights and values. Modern public video surveillance systems consist of networks of linked cameras spread over vast portions of public space. These cameras can be equipped with technologies like high resolution and magnification, motion detection, infrared vision, and biometric identification—all linked to a powerful network capable of automated tracking, archiving, and identifying suspect behavior. These types of systems are beginning to cover the American urban landscape, from metropolises like Chicago and Washington, D.C. to cities and towns like Virginia Beach and Cicero, Illinois.

It is understandable that American cities and their law enforcement officers place great emphasis on developing new tools to confront the increased threat of terrorism faced by Americans in the twenty-first century—and the apparent value of surveillance footage in the investigation into the July 2005 bombings in London only strengthens the appeal of this particular tool. Likewise, it is understandable that authorities would want to use any available means to prevent or deter other serious threats to public safety. But the value of modern video surveillance must be balanced with the need to protect our core constitutional rights and values, including privacy and anonymity, free speech and association, government accountability, and equal protection. The new technologies may help protect the public, but they also enable authorities to more deeply intrude upon these rights. Lawmakers can no longer rely on constitutional law and technological limits—they need to proactively seek ways to harmonize constitutional rights and values with the new surveillance capabilities. We believe that constitutional rights and values can be reconciled with law enforcement and anti-terrorism goals, but officials often lack the resources to properly gauge how to achieve such reconciliation.

The Constitution Project's Liberty and Security Initiative has therefore formulated guidelines to assist local and state officials charged with authorizing, designing, and managing public video surveillance systems. These guidelines will help communities meet the challenge of reconciling Americans' strong and legitimate interest in protection against terrorism and other dangers with their longstanding and constitutionally-enshrined commitment to individual freedom. In addition, these guidelines can lower the overall cost of a video surveillance system by identifying unnecessary or ineffective aspects of the design and reducing the likelihood of legal challenge to public video surveillance.

In summary, our recommended guidelines for public video surveillance systems are as follows:

I. Core Principles Governing the Creation and Design of Public Video Surveillance Systems

1. Create a public video surveillance system only to further a clearly articulated law enforcement purpose.

2. Create permanent public video surveillance systems only to address serious threats to public safety that are of indefinite duration.

3. Ensure that public video surveillance systems are capable of effectively achieving their articulated purposes.

4. Compare the cost of a public video surveillance system to alternative means of addressing the stated purposes of the system.

5. Assess the impact of a public video surveillance system on constitutional rights and values.

6. Design the scope and capabilities of a public video surveillance system to minimize its negative impact on constitutional rights and values.

7. Create technological and administrative safeguards to reduce the potential for misuse and abuse of the system.

8. Ensure that the decision to create a public video surveillance system, as well as major decisions affecting its design, are made through an open and publicly accountable process.

II. Publicly Accountable Procedures for Establishing Public Video Surveillance Systems

1. For permanent or long-term public video surveillance systems, conduct a civil liberties impact assessment and overall cost-benefit analysis through a public deliberative process that includes community input.

2. For temporary public video surveillance systems, demonstrate to a neutral magistrate that the system has no greater scope or capabilities than reasonably necessary to achieve a legitimate law enforcement purpose.

III. Principles and Rules for Use of Public Video Surveillance Systems

1. Once a public video surveillance system is authorized, no additional approval is necessary to use the capabilities of the system for "observation."

2. "Record" footage from public video surveillance systems only to the extent necessary to further the system's stated purposes.

3. Under most circumstances, individuals may be "tracked" or "identified" by a public video surveillance system only pursuant to a warrant: (a) law enforcement must obtain a warrant prior to using a public video surveillance system to track or identify an individual; (b) law enforcement must obtain a warrant prior to using a "watch list" to automatically identify individuals, except when using a federal anti-terrorism watch list.

4. A public video surveillance system may be used for legitimate law enforcement purposes other than its original purpose, subject to certain restrictions: (a) no additional approval is required for incidental use of the system; (b) law enforcement must obtain administrative approval for secondary use of "pre-archival" stored video surveillance footage; (c) law enforcement must obtain a warrant for secondary use of "archival" stored video surveillance footage.

5. Employ technological and administrative safeguards to reduce the potential for misuse and abuse of the system: (a) provide safeguards for use of stored video surveillance data; (b) provide safeguards for personnel with access to a public video surveillance system; (c) provide public notice of surveillance where appropriate.

6. Prohibit, to the extent possible, sharing of public video surveillance data with third parties, including private litigants, and restrict sharing with other governmental entities.

7. Establish mechanisms to protect the rights of identifiable individuals captured on video surveillance data.

8. Apply to any law enforcement use of privately collected video surveillance data the same standards that apply to public video surveillance data.

9. Provide appropriate remedies for those harmed by misuse or abuse of public video surveillance systems.

GUIDELINES FOR PUBLIC VIDEO SURVEILLANCE

I. Introduction

Within days of the July 2005 bombings on London's subway and bus system, authorities had identified the bombers, retraced their paths, and detained suspected accomplices thanks in part to footage from London's elaborate public video surveillance system. While the cameras did not prevent the attacks, their value in the subsequent investigation has reinvigorated movements, both in the United States and elsewhere, to develop similar systems. From Washington, D.C. to Paris, France to Cicero, Illinois, local officials are expressing renewed interest in video surveillance. And this surveillance is a far cry from the simple closed-circuit camera systems employed by law enforcement agencies in the past. Officials concerned about terrorist and other serious threats are seeking public video surveillance systems that are pervasive, intelligent, and outfitted with the latest technologies.

The potential of video surveillance has generated interest among state and local law enforcement officials,* who see video surveillance as a cost-effective and unobtrusive means of combating serious threats to public safety. Many civil libertarians and privacy advocates, in contrast, believe that pervasive government surveillance, which will inevitably capture the activity of law-abiding people, is antithetical to the ideals of a society that values individual rights, autonomy, and freedom from government intrusion. Reconciliation of these important concerns demands the serious attention of citizens, lawmakers, law enforcement agencies, and eventually the courts.

* We intend these guidelines to be used by state and local officials and law enforcement agencies. Federal authorities, whose jurisdiction includes national security, border regions, and other anomalous areas, will find many of the recommendations in this document to be inapplicable. Nevertheless, we invite federal officials to apply the principles of this document to the extent feasible.

As we use the term here, a "public video surveillance system" is a camera network administered by or for law enforcement to monitor activities in a public place or places.* At its simplest, it is nothing more than a small network of cameras that allows an officer to quickly scan current activity in an area. At its most complex, such a surveillance system can include hundreds or thousands of cameras—equipped with technologies like high resolution and magnification, motion detection, infrared vision, and automated identification—all linked to a powerful network capable of automated tracking, archiving, and identifying suspect behavior. What was once the grist of science fiction novels is quickly becoming the reality of modern law enforcement.

Without question, the legal and social implications of surveillance networks are vast. To protect the spirit of our most important constitutional rights and values, assuage public fears of "big brother," and manage liability, public video surveillance systems must be designed narrowly, used carefully, and examined thoroughly. At the same time, effective public video surveillance systems should not be abandoned merely because they can be abused. We believe that constitutional rights and values *can* be reconciled with law enforcement and anti-terrorism goals, but officials often lack the resources to properly gauge *how* to achieve such reconciliation. To that end, the Constitution Project's Liberty and Security Initiative offers these guidelines for public video surveillance programs.

II. Background

As the legal, social and technological issues surrounding video surveillance are complex, this section provides necessary background. We briefly examine the status of video surveillance in its modern manifestation: large-scale, long-term, pervasive camera networks capable of rendering a city center into the surveillance equivalent of a bank lobby. We also discuss the technologies of modern video surveillance, from "pan, tilt, and zoom" to automated information based on biological features ("biometric" identification) to intelligent networks, as well as the terrorism threats that spurred their development and deployment. This section also discusses the constitutional rights and values implicated by public video surveillance systems and the existing legal status of such surveillance.

* While the principles we describe can aid those concerned about the private deployment of surveillance cameras, such as in a mall or theme park, these guidelines are not aimed directly at private surveillance. If, however, a privately created surveillance system or footage from one is made available to law enforcement, it should be treated as public for the purposes of these guidelines. These guidelines also do not address law enforcement surveillance of non-public places, which is subject to a variety of additional legal restrictions.

A. Developments in and Use of Video Surveillance

Modern public video surveillance systems do not lack antecedents. Cities first experimented with mounting cameras over public streets in the 1960s.[1] And, while most early camera installations have been removed, police have continued to make selective use of public video cameras to gather evidence from a specific place or individual in the course of an investigation. Also, as the famous images of the September 11th hijackers illustrate, law enforcement has used extensive footage from privately operated monitoring cameras—such as those on ATMs, in convenience stores, and in airports. In recent years, driven by concerns regarding terrorism and improvements in technology, cities and communities have begun to install the next generation of video surveillance—pervasive networks of cameras equipped with the latest high-tech features.

1. The threat of terrorism

As the reaction to the July 2005 attacks in London demonstrated, the increased threat of terrorism over the last several years has drastically changed the perceived value of video surveillance systems. Terrorism is both quantitatively and qualitatively different from other criminal threats. In terms of physical cost, damage to life and limb, and long-term social impact, the potential costs of terrorism far outstrip those of all but the most virulent crimes. Moreover, while criminals and zealots have resorted to terrorism for centuries, the potential impact of terrorist attacks has increased exponentially in modern society. Dense urban environments, public reliance on vital and sensitive infrastructure, and the accessibility of weapons of mass destruction each multiply the dangers of terrorism.

In response, law enforcement agencies around the world, including here in the United States, are increasingly seeking systems like the one in London—a vast network, with constant monitoring of likely "targets," automated identification of suspected terrorists or suspicious activity, and the ability to track individuals from location to location.[2] Indeed, the London system itself was deployed largely to combat the earlier terrorist threat of the Irish Republican Army.[3] These systems are a far cry from those of even a few years ago, when public video surveillance was primarily a selective law enforcement tool—used on a temporary basis at certain times and places to track known individuals.

2. New technology

The ability of new camera and network technologies to identify, track, and investigate the activities of formerly anonymous individuals fundamentally changes the nature of video surveillance. While the various technological developments overlap, for these guidelines we conceive of four distinct types of surveillance technologies, each of which calls for differing rules and restrictions (*see* Sections III.C.1.–3., *infra*): (a) observation technologies; (b) recording technologies; (c) tracking technologies; and (d) identification technologies. A final section discusses technologies that may be employed to *mitigate* the impact of surveillance on constitutional rights and values.

a) Observation technologies

The ability of video cameras to observe has developed significantly. Early closed-circuit surveillance cameras—and the ones still used by many private and public entities—can "see" about as far as a human eye but with a narrower field of view. Modern cameras, in contrast, can pan and tilt at the direction of controllers to expand their effective coverage area, and magnification can exponentially improve the detail that camera images can render. With a mere 60-times optical zoom lens, a camera "can read the wording on a cigarette packet at 100 yards;"[4] some cities are reportedly deploying cameras capable of 400-times magnification.[5] Other observation technologies allow cameras to render usable images in very low light, and infrared "night-vision" technology can render clear images with no visible light whatsoever.

b) Recording technologies

In addition to lowering storage costs and improving the quality of recordings, the advent of digital video technology permits manipulation of recorded video data in ways impossible with analog recordings. First, digital video records can be supplemented with "metadata:" information about the recording itself or the captured images that increases the usefulness of the recording. For instance, records from cameras filming an urban financial district could be supplemented with date, time, location, summary data concerning numbers of people or automobiles, or even information about recognized individuals—such as criminal records or previous visits to the same location. Second, recorded digital footage may also be searched more cheaply and easily than analog footage. Combined with rich metadata, a database of video footage could be searched for specific individuals or activity matching a specified pattern, or used to create a "digital dossier" about an individual.[6] Perhaps more importantly, law enforcement can instantly review footage from any time and location that exists in the database.

c) Tracking technologies

Today's cameras and camera networks can also be equipped with technology allowing them to track movement in their field of view or across networked cameras. Not only can simple motion sensors enable a camera to activate when it detects motion, but more advanced technology can allow the camera to automatically track an object moving through its field of view. Combined with pan, tilt, and zoom technology, such a camera could track a person walking the length of entire city blocks, around corners, or from a storefront to a vehicle.

Moreover, software can be added to the systems running the cameras to enable more sophisticated tracking, identification of suspicious or unusual movement, and deduction of useful data such as speed, path, and destination. In contrast to the popular image of a lone security guard watching a bank of grainy monitors, systems commercially available today can provide a unified, virtual-reality perspective of a monitored area—similar to the interface of the popular Google Earth software[7]—allowing an operator to automatically follow an object as it moves from camera view to camera view. In real time or using stored data, law enforcement can actively and pervasively track specific individuals or activity in large areas, or even be notified if the system detects unusual activity.[8]

d) Identification technologies

Automated identification software continues to improve. Traditionally, identification was not a central purpose of video surveillance because law enforcement officers already knew the identity of the individual or individuals they were monitoring. Even where authorities sought to identify a suspect caught on video, they generally solicited citizen aid.[9] This is changing. Already, video surveillance of license numbers can identify individual cars: London has supplemented many of its downtown cameras with technology that automatically captures and analyzes drivers' license plates—a technology increasingly employed across the U.K.[10] Radio-frequency identification, already used in employee badges and "E-ZPass" systems, can be employed in conjunction with surveillance systems as well.[11]

Facial recognition systems, while far from perfect, are steadily improving in quality as recent advances increase the reliability of the identification process.[12] These technologies are attractive to law enforcement agencies, which hope to be able to automatically check videotape for suspects the way fingerprints at a crime scene can be automatically checked against a database of known criminals. Beyond the fingerprint analogy, moreover, facial recognition may one day be used to quickly and cheaply create a catalog of an individual's every movement through a surveilled area. Members of Congress and other officials have shown interest in using biometric identification, such as facial recognition and iris scanners,

to identify individuals on terror watch lists,[13] but smaller-scale facial recognition systems are already in place. Virginia Beach, for instance, used facial-recognition devices in its permanent boardwalk video surveillance system.[14] New York has reportedly contemplated installing numerous biometric recognition devices in Times Square.[15] Perhaps most famously, security for the 2001 Superbowl included hundreds of facial recognition cameras.[16]

e) Technologies that can mitigate the impact of surveillance

Conversely, there are also technologies that can mitigate the invasive effects of those described above. Some technologies simply help limit the information captured. For instance, cameras can be programmed so that they cannot pan or tilt in ways that would reveal private spaces, such as looking through windows into private residences. Similarly, "digital masking" technology can automatically hide the faces of non-targeted individuals on recorded footage.[17] Other technologies can help authorities effectively protect recorded data from unauthorized use or disclosure. Stored data can be supplemented with encryption technology, which permits only those with the proper decryption "key" to unscramble the stored footage. Other means of data authentication, such as a digital "watermark," do not prevent access to recorded footage, but can be used to create a record of when and where data is accessed.

3. Expansion of scale, permanence, and prevalence of public video surveillance

The confluence of the increased threat of terrorism and new, more powerful technologies has spurred a dramatic growth not only in the prevalence of public video surveillance systems, but in their scale and scope as well.

In the past few years, many American cities and public organizations have come to view public video surveillance not merely as a tool for specific investigations, but as something that might be a permanent feature of public space. Looking to the example of London, American cities such as Washington, D.C. and Chicago have made similar plans to install networks of cameras. To address terrorist threats, these networks are being designed to cover transportation networks, business districts, public areas, monuments and government buildings, and other vital infrastructure.[18] Chicago's surveillance network may be the nation's most extensive and advanced, making its residents "some of the most closely observed in the world."[19] The city has built a massive, 1000-mile fiber-optic grid equipped "with cameras and biochemical sensors to watch for signs of terrorism, crime and traffic tie-ups."[20] The system is reportedly linked to software that can automatically alert police whenever an individual near a sensitive location "wanders aimlessly in circles, lingers outside a public building, pulls a car onto the shoulder of a highway, or leaves a package and walks away from it."[21] Other cities,

such as Baltimore, Maryland, Cicero, Illinois, and Newport, Rhode Island, are reportedly using federal anti-terrorism grants to build similar, if smaller, camera networks.[22]

The rapid expansion of public video surveillance has sparked a fierce debate over the efficacy of the systems in fighting crime. A 2003 review by the Office of the Information and Privacy Commissioner of Alberta, Canada found the consensus amongst empirical studies to be that video surveillance has little effect on violent crime, and only a small positive effect on property crime.[23] This positive effect on property crime, moreover, was substantially less than the effect of improved lighting.[24] Also unclear is the effect of other simultaneous public-safety enhancements—such as improved street lighting—and the extent to which criminal activity was simply displaced to non-surveilled areas. Finally, given the cost of deploying, maintaining, and operating such systems, no data exists to demonstrate that video surveillance is a more effective use of public resources than traditional law enforcement.

Given such evidence, some cities have abandoned video surveillance plans. According to the American Civil Liberties Union (ACLU), officials in Detroit, Michigan contemplated the use of generalized video surveillance for 14 years, but ultimately concluded that high maintenance and personnel costs could not justify the limited results.[25] In Oakland, California, the ACLU reports that the police department, after lobbying for three years for surveillance cameras in public places, eventually concluded that "there is no conclusive way to establish that the presence of video surveillance cameras resulted in the prevention or reduction of crime."[26]

While these studies and examples are grist for those who oppose video surveillance, the conclusions they draw by no means end the debate. Anecdotally, video surveillance has aided the investigation into high-profile crimes, and many cities and communities report their satisfaction with public video surveillance systems. In addition, no study to date tracks the effect of surveillance on terrorism. While suicidal terrorists are unlikely to be deterred by video surveillance, the technology may aid in the prevention and investigation of attacks. At the least, however, the mixed nature of the evidence should encourage any jurisdiction considering use of video surveillance to review existing literature, carefully weigh the monetary costs and social impact against the benefits of video surveillance, and engage in limited trials prior to full-scale implementation.

B. Constitutional Rights and Values at Stake

Public video surveillance systems implicate many fundamental values. This section identifies the range of constitutional rights and values at stake in the debate over public video surveillance.

1. Privacy and anonymity

Privacy is a general term, covering concepts that are often very different from one another. Privacy includes "informational privacy" rights, such as a consumer's right to keep the businesses she patronizes from disclosing her name and address, "decisional privacy," which includes such matters as reproductive decisions, and the more traditional "physical privacy" over one's self and property. Though these different branches of the privacy right are conceptually separable and vary in their legal protection, they all center on the right to personal autonomy—what Justice Brandeis famously called "the right to be let alone."[27] We use the term "privacy" in this broad sense.

Closely related to privacy is the right to anonymity. Alan Westin, author of a seminal privacy treatise, described anonymity as a form of privacy that "occurs when the individual is in public places or performing public acts but still seeks, and finds, freedom from identification and surveillance."[28] Because of this anonymity, "he does not expect to be personally identified and held to the full rules of behavior and role that would operate if he were known to those observing him."[29] The Supreme Court has validated this view by recognizing that people should be able to remain anonymous while exercising certain constitutionally protected rights.[30] Anonymity remains a fundamental freedom even as urban environments and technology increasingly allow government or other interested parties to identify every passerby.[31]

Few would disagree that public video surveillance systems have the potential to be used in ways that infringe on privacy and anonymity rights. Commentators often erroneously assume that there is "no reasonable expectation of privacy" in streets or parks or other areas open to view.[32] However, despite the legal doctrine relied on, this is false as an empirical matter. Most people expect to remain anonymous in many "public" contexts, such as entering an Alcoholics Anonymous meeting, a psychiatrist's office, an infertility clinic, or the headquarters of a fringe religious or cultural group. Similarly, even when they are in a public place, most people expect to keep private the information that might be detectable from such sources as the exposed words on a vial of prescription drugs, the moving lips of a couple engaged in hushed conversation, or diary entries written by a person sitting on a park bench. Ubiquitous, technologically-enhanced video cameras could enable the government to routinely capture footage of all of these activities.

2. Freedom of expression and association

As the First Amendment attests, our society has a deep commitment to preserving the right of individuals to freely express their ideas and to associate freely to share those ideas. To

protect this freedom, even laws or policies that merely "chill" free expression or freedom of association may be struck down.[33] The Supreme Court has recognized that the ability to freely express oneself or associate includes the right to do so without revealing one's identity.[34] A sufficiently powerful public camera could endanger these rights by giving the government an extensive record of what individuals say and read, and with whom they associate.[35]

3. Government accountability and procedural safeguards

Equally central to the concept of a free society is the principle that laws—rather than people—govern us. We submit to society's laws knowing the authorities must do the same. Through representatives, the public enacts rules and procedures that dictate when the government can deprive any individual of life, liberty, or property. The Fifth and Fourteenth Amendments' specific guarantee of "due process" is one aspect of this right, but it pervades all aspects and all levels of American society—requiring that government remain accountable to the governed. Open government or "sunshine" laws, notice requirements, and regular elections are all manifestations of this social value. Of course, central to this principle is the ability of the public to know if the government is adhering to its own rules and how it reaches its decisions.

Pervasive public video surveillance systems could allow officials to evade both procedural safeguards and accountability. The disclosure in December 2005 of the National Security Agency's warrantless domestic surveillance program highlighted the critical need to maintain such controls. As the Constitution Project's Liberty and Security Initiative and many others have pointed out in connection with the NSA surveillance program, it is essential that government surveillance be conducted only with independent oversight and as part of a system of checks and balances.* In the public video surveillance context as well, unless procedural limits are implemented, law enforcement officers might use video surveillance to improperly monitor private activity or otherwise go beyond the bounds of their authority. Without accountability safeguards, moreover, the officers might never have to explain their actions.

* In December 2005, the Liberty and Security Initiative released a statement criticizing the recently disclosed NSA warrantless surveillance program and refuting the Administration's legal justifications for the program. The statement also noted that: "Although we fully agree that the president must be able to take action to protect our nation from the threat of terrorism, he must do so in a manner consistent with the rule of law, our commitment to civil liberties, and our constitutional system of checks and balances." Statement available at: http://www.constitutionproject.org/pdf/1_5_updated_statement.pdf. In addition, on February 28, 2006, the Constitution Project and the Center for National Security Studies filed an *amicus* brief in the Foreign Intelligence Surveillance Court analyzing the legal failures of the NSA's warrantless surveillance program. Brief available at: http://www.constitutionproject.org/pdf/FISC_memorandum.PDF.

4. Equal protection and anti-discrimination

American society and law abhor discrimination for many reasons. Discrimination degrades its victims and also reinforces one of the heinous and most anti-American of social institutions: a class structure. Moreover, discrimination retards the very ability of any insular minority group—be it religious, racial, cultural, political, or ethnic—to participate fully in civil society. In *United States v. Carolene Products Co.,* Justice Stone famously suggested that "prejudice against discrete and insular minorities may be a special condition, which tends seriously to curtail the operation of those political processes ordinarily to be relied upon to protect minorities."[36] This idea paved the way for much of modern Equal Protection and Due Process Clause jurisprudence.

The potential for discriminatory use by government officials is a significant problem for any video surveillance system. The British, who administer the largest video surveillance systems of any democratic nation, admit that some degree of ethnic, racial, and gender profiling exists. Two experts from the Centre for Criminology and Criminal Justice at Hull University in Britain found that, based on data from the city of Hull's surveillance system, "[b]lack people were between one-and-a-half and two-and-a-half times more likely to be surveilled than one would expect from their presence in the population."[37] Disproportionate surveillance of, for instance, young black men can lead to a false perception amongst law enforcement of that population's criminality. Discriminatory use of surveillance can also give ammunition to those with salacious or malicious agendas: British officers have been caught offering for sale voyeuristic videos of women caught on surveillance tapes;[38] in Washington, D.C., a well-known police lieutenant was charged with using police databases to blackmail married patrons of gay establishments.[39] While hopefully such behavior is rare, it illustrates the discriminatory potential of video surveillance.

C. Existing Law and Regulatory Proposals

Legal authorities governing use of public video surveillance are sparse, and laws governing modern, technologically advanced public video surveillance systems are rarer still. Statutes and regulations generally lag behind technological development. Constitutional law typically develops at an even more glacial pace. While many laws and constitutional doctrines have important implications for public video surveillance, a review of these laws highlights the inadequacy of existing law and regulatory proposals to properly address the balance between security interests and implicated rights, liberties, and social values.

1. Constitutional law

Video surveillance implicates several constitutional doctrines—generally centered on the First and Fourth Amendments. The Fourth Amendment protects individuals from "unreasonable searches and seizures," but no court has yet found law enforcement use of video cameras to surveil activity on public property to be an unreasonable search. While the Supreme Court has recognized that "people are not shorn of all Fourth Amendment protection when they step from their homes onto the public sidewalks"[40] and that constitutional privacy interests may well be implicated when a camera is focused on activities the government has no legitimate interest in monitoring, such as "a class ring" or "identifiable human faces,"[41] it has not extended protection to cover the routine use of video surveillance. Many lower courts have in fact claimed that one cannot have a reasonable expectation of privacy in public areas.[42] This conclusion may be based on the fact that, until recently, authorities could not easily deprive people of the seclusion of an isolated public space or the anonymity of a crowded street. Doing so would have required authorities to target a particular individual, conceal their own presence, and track her movements.

Similarly, courts have not yet recognized that modern video surveillance may chill or otherwise intrude upon protected First Amendment activities. First Amendment jurisprudence does acknowledge the special role of public places in expressive activity,[43] and forbids laws or policies that disproportionately burden expression in such places,[44] but "neither the speech or association guaranties are likely to provide a basis for constitutional regulation of most public surveillance, at least when it is visual only."[45] The Supreme Court rejected, for instance, a claim by Vietnam-era antiwar protesters that their extensive surveillance dossiers, collected by the Army, chilled their ability to freely express themselves.[46] Thus, while little question exists that the values and liberties that undergird the First and Fourth Amendments can be violated by overzealous video surveillance, the jurisprudence to this point has been very permissive.

2. Federal statutes

A few federal laws peripherally affect public video surveillance, but none substantively limit law enforcement's use of cameras. The Electronic Communications Privacy Act (ECPA), which limits law enforcement or private parties' ability to intercept or access private communications, applies only to "aural" communications—and thus does not apply to video surveillance lacking sound.[47] Even footage *with* sound may not trigger ECPA, as claimants would still have to demonstrate a reasonable expectation of privacy in the intercepted conversation.[48] Federal anti-terrorism and foreign intelligence laws, including the USA PATRIOT Act and the Foreign Intelligence Surveillance Act (FISA), not only fail to limit

government use of video surveillance, they in fact streamline intergovernmental sharing of surveillance data in any investigation relating to terrorism.[49] The Freedom of Information Act (FOIA), which requires the federal government to make information available to the public, may also be a legal means through which surveillance data on individuals could be released to the public, though the law contains a privacy exception that may prevent disclosure to private parties.[50]

Though they lack the force of federal law, the influential "Fair Information Practices" originated in recommendations written by the United States government.[51] The Fair Information Practices provide helpful guidance for the treatment of any governmental-held record containing personally identifiable information, and have served as the model for much of international law on personal data, including the 1995 European Union Data Protection Directive.[52] In their most basic form, the Fair Information Practices require that individuals be provided the following rights with respect to the collection, use, or transfer of their personal information:

- **Notice and awareness** of the purpose of data collection, and how such information is used;
- **Consent** to the collection of personal information, and choice concerning how it is used;
- **Access to and participation in** the process of data collection and use, including the right to correct errors;
- **Integrity and security** adequate to protect the information against loss or misuse; and
- **Redress and accountability** for injury resulting from loss or misuse of personal information.

3. State law

Several state statutes regulate aspects of public use of video surveillance. In New York, for example, video surveillance can only be conducted as part of a police investigation into the allegedly criminal behavior of an individual pursuant to a warrant. Because of what the statute terms "the reasonable expectation of privacy under the constitution of this state or of the United States," the bar for authorizing or approving such a warrant is set quite high, and the alleged crimes must be quite serious.[53] Arizona, in contrast, merely makes it a misdemeanor for a person to use video "surveillance" in a public place without posting notice.[54] The laws of other states vary, and while any authority seeking to adopt such a system should investigate applicable law, state statutes generally affect video surveillance only in cursory fashion, if at all.

4. Regulatory Proposals

These guidelines are not the first attempt to propose a regulatory framework for public video surveillance. In 1999, the American Bar Association (ABA) published standards for technologically-assisted physical surveillance, including video surveillance, as part of the Third Edition of the *ABA Standards for Criminal Justice, Electronic Surveillance (ABA Standards).*[55] These standards stress that while crime-fighting may benefit substantially from video surveillance and other "technologically-assisted physical surveillance," such as satellite tracking or use of chemical detection devices,[56] such technologies "can also diminish privacy, freedom of speech, association and travel, and the openness of society."[57] The *ABA Standards* propose a number of principles aimed at ensuring that such potentially invasive technologies are not used arbitrarily, in a discriminatory fashion, or in ways that intrude upon privacy or "First Amendment freedoms and related values" more than is necessary to achieve their "legitimate law enforcement purpose."[58] They also stress that such surveillance be subject to mechanisms of democratic accountability.[59] While the *ABA Standards* are a valuable tool and arrive at many similar conclusions as this document, they are incomplete—as both the 2001 terrorist attacks and most of the technological developments discussed above post-date their publication.

Many Canadian provinces have published guidelines for use of public video surveillance, pursuant to Canadian privacy laws that require various safeguards for any collection or use of personal information.[60] Based on the Fair Information Practices, these guidelines recognize the danger to privacy posed by video surveillance, and require procedures to curb those dangers. The Alberta guidelines, for example, cover any surveillance that collects information about identifiable individuals; require surveillance proposals to be subjected to efficacy analysis and a "privacy impact assessment;" and limit who may access and use stored records and for what purposes.[61] Though specific to their respective provinces and based on Canadian law, several provisions of these guidelines could be productively incorporated into a more thorough system of rules under United States law.

A few other political entities have also proposed guidelines for regulating law enforcement use of video surveillance. The government of New South Wales, Australia, published in 2000 guidelines aimed at cities under its jurisdiction, including Sydney.[62] The New South Wales guidelines recommend a number of steps to protect civil liberties, including community consultation, limited access to video footage, monitoring, and regular audits. In the United States, the city council of Washington, D.C. introduced rules in 2002 to govern how the city should use its video surveillance system going forward.[63] These models provide a helpful starting point or supplement for other cities or communities considering public video surveillance systems, though they are not comprehensive and are specific to their own jurisdictions.

III. Guidelines for Public Video Surveillance

The above background reveals several deficiencies in the resources available to American communities to address the benefits, dangers, and costs of modern public video surveillance. First, public video surveillance systems are fundamentally different—in terms of goals, capabilities, and scope—than the video surveillance systems of the past. Second, while the post-9/11 world requires innovative security measures, authorities must understand that public video surveillance systems pose new and more serious threats to constitutional rights and values than the surveillance cameras of the past. While any government-run camera can be used to infringe privacy or evade procedural limits, modern surveillance networks can also eliminate much of the privacy and anonymity individuals take for granted; chill a substantial amount of free expression; inhibit people from freely associating with others; create an unaccountable, unsupervised means of constant monitoring; and become a tool for discrimination against unpopular minority groups. Finally, existing law and regulatory proposals are insufficient to adequately cope with these threats. To address these deficiencies, the Constitution Project's Liberty and Security Initiative proposes the guidelines that follow. While technology and social factors will continue to evolve, these guidelines allow any state, city, or community considering a public video surveillance system to develop a robust and effective regime that simultaneously protects the core constitutional rights and values of its residents, avoids potential liability stemming from infringement of these rights, and still permits law enforcement to fully address the real and dangerous threats of the modern world.*

Section A of the guidelines discusses core principles that should govern the creation and design of public video surveillance systems. These principles should help a community determine whether a surveillance system should be deployed at all, where it should be installed, its capabilities, and the procedural and substantive rules that protect against misuse and abuse. Section B outlines two specific procedures through which these substantive issues may be examined and resolved in a publicly accountable manner: (1) a detailed, participatory, and transparent process that includes a "civil liberties impact assessment" and a cost-benefit analysis to assess proposals for permanent, large-scale public video surveillance systems; and (2) a streamlined process involving judicial oversight and approval designed for shorter-term public video surveillance systems that must be implemented either quickly or

* As stated in Section I, while the principles we describe can aid those concerned about the private deployment of surveillance cameras, such as in a mall or theme park, these guidelines are not aimed directly at private surveillance. If, however, a privately created surveillance system or footage from one is made available to law enforcement, it should be treated as public for the purposes of these guidelines. These guidelines also do not address law enforcement surveillance of non-public places, which is subject to a variety of additional legal restrictions.

in secret. Section C sets forth rules and procedures to ensure that the use of a system, once installed, is aligned with core substantive principles. This section discusses technical and administrative constraints on the use of surveillance systems, including the retention of data, the identification of surveilled individuals, the deployment of enhanced technologies, and the rights of individuals captured on camera.

A. Core Principles Governing the Creation and Design of Public Video Surveillance Systems

This section outlines the core principles that should be considered throughout the lifecycle of a public video surveillance system, including: the purposes that justify its creation; the necessity of evaluating cost, efficacy, and the impact on constitutional rights and values; articulation of the coverage and capabilities of the system; and the creation of procedural and substantive safeguards to protect against misuse and abuse.

1. Create a public video surveillance system only to further a clearly articulated law enforcement purpose.

The initial step in the creation of a public video surveillance system is a clear statement of the legitimate law enforcement purpose or purposes for the system. This statement of purpose provides context for both the analysis of the system's social impact and economic cost and benefits before its installation (*see* Section III.B., *infra*), and its regulation subsequent to installation (*see* Section III.C., *infra*). The governmental body seeking to create the system must articulate its purpose as clearly and specifically as practicable to enable the public or reviewing body to assess the legitimacy of the stated purpose and evaluate the system's design and use. The statement of purpose provides several important benefits:

- It allows members of the affected communities to evaluate the legitimacy of the purposes and consider whether they are likely to be furthered by a public video surveillance system.
- Should the purposes be deemed valid, the statement then informs every aspect of the design—including whether the system should be permanent or temporary, the locations where it should be installed, the technological features it should embody, and the rules that govern its use. Only a system capable of achieving its purposes should be considered for installation (*see* Section III.A.3., *infra*).
- It provides a means for holding government publicly accountable for any failure of the system to serve or achieve its purposes.

- It allows the public to identify and punish individual abuse and misuse of the system by forcing officials to justify their use with respect to the purposes of the system.

2. Create permanent public video surveillance systems only to address serious threats to public safety that are of indefinite duration.

The risk of harm to constitutional rights and values posed by a public video surveillance system increases with its duration. The longer a system operates, the more activities and information it captures—permitting more and greater violations of privacy and anonymity and correspondingly higher probability of public outcry and legal liability. Moreover, the knowledge that surveillance is an enduring feature of the public landscape may inexorably render such spaces less suitable for the exercise of free speech and other liberties. Permanent systems, which maximize the potential for such violations, should be created only to address serious threats to public safety that are of indefinite duration.

While every community may reach its own conclusion as to which threats are "serious" and "of indefinite duration," we conclude that, in general, the only law enforcement concerns that meet this test are (1) a persistent threat of terrorist attack or (2) danger to critical public infrastructure and the people who surround such sites. The threat of terrorism, which regrettably appears to be an enduring feature of the modern world, certainly rises to the level of serious and of indefinite duration for those communities with good reason to believe they may be attacked.* In addition to terrorist threats, danger to critical public infrastructure, both criminal and accidental, poses long-term risks to public safety requiring the utmost caution and preventative efforts. Such infrastructure includes public transportation networks, major traffic arteries and interchanges, and public utility facilities.

By contrast, we conclude that property crime and violent crime other than terrorism, regardless of seriousness, do not pose a threat of indefinite duration at any given location. While communities must be able to prevent and respond to these threats to public safety, we urge employment of other investigative or prophylactic means less intrusive than permanent surveillance systems—including additional policing or, if justified, a temporary public surveillance system. This recommendation is buttressed by evidence that public video surveillance has not been a cost-effective means of combating property and violent crime (*see* Section II.A.3., *supra*). Should a community conclude differently, however, we urge officials to nevertheless apply the seriousness and indefiniteness criteria to determine which threats

* Of course, while many communities may be understandably fearful of terrorist attack, each community must dispassionately assess the reasonability of its fears. This determination should be based on considerations such as the character of the location, its symbolic or strategic value, its role as critical public infrastructure, and specific threats or intelligence.

warrant the creation of permanent surveillance systems, as well as the remainder of these guidelines.

3. Ensure that public video surveillance systems are capable of effectively achieving their articulated purposes.

A public video surveillance system must be effective in addressing the stated purposes for which it was created. In light of the constitutional rights and values at stake, the costs of such a system, and the legal risks it poses, a community should carefully assess whether a video surveillance system is an effective means of combating the particular threats that justified its creation. For instance, an anti-terrorism system that contains automated identification features, yet lacks trained personnel who understand how to take full advantage of the specialized software, may not be effective or justify its continued use. Similarly, a system created to combat crime at night in a public park may not be effective if it is not equipped with low-light technology. As the *ABA Standards* note, a surveillance technique as powerful as video surveillance "should be capable of doing what it purports to do."[64]

Section B of the guidelines describes methods of assessing the efficacy of public video surveillance systems. In general, however, communities and officials should contemplate the efficacy of the system at the design stage, upon installation, and after the system has been in use. Each location, as well as the system as a whole, should be assessed. A community should also review existing data concerning the efficacy of such systems (*see* Section II.A.3., *supra*), investigate the experiences of similar cities and communities with public video surveillance systems, and consider limited trials followed by review prior to large-scale installation.

4. Compare the cost of a public video surveillance system to alternative means of addressing the stated purposes of the system.

A community considering a public video surveillance system must consider its cost* in comparison to alternative uses of those same resources. If a surveillance system consumes more resources than alternative means of addressing its articulated purposes, then—all else being equal—the community should direct its resources toward the cheaper alternative. For instance, if the resources necessary to purchase, install, and operate a public video surveillance system could employ ten additional police officers, the community should evaluate whether those ten officers, if deployed in the targeted area, could achieve the law

* While any negative impact of video surveillance on constitutional rights and values is also a "cost," we use the term in the economic sense to refer only to monetary or resource costs. The term "cost-benefit analysis," however, refers to both social and economic costs.

enforcement objectives as well or better than cameras. Alternatively, a mix of some new officers and more limited video surveillance may provide the most return on the community's investment.

5. Assess the impact of a public video surveillance system on constitutional rights and values.

While few law enforcement authorities would implement video surveillance in public places with the intent to infringe upon the constitutional rights and values of their communities, nevertheless the importance of those rights and values demands careful attention to the unintended effects of surveillance systems in the design of public video surveillance systems. These social "costs," though more difficult—if not impossible—to quantify, are as important a factor in evaluating the design and use of public video surveillance as calculation of economic costs.

As described more fully in Section II.B., *supra*, public video surveillance implicates a number of important constitutional rights and values. Communities should consider and articulate the impact of the planned public video surveillance system on each of the following:

- **Privacy and anonymity** rights are clearly imperiled by public video surveillance systems, if misused. Cameras could routinely capture footage of individuals engaging in activities in which most expect anonymity, such as entering an Alcoholics Anonymous meeting, a psychiatrist's office, or the headquarters of a fringe religious or cultural group. Similarly, cameras might capture things most people would seek to keep private, such as the label on a vial purchased at a drug store or an intimate conversation between two family members on a stroll.
- **Freedom of speech and association** are similarly at risk. A sufficiently powerful public camera could give the government an extensive record of what individuals say and read, and with whom they associate outside of the home—substantially "chilling" the ability or desire of individuals to engage in protected conduct.
- **Government accountability and procedural safeguards** that preserve the relationship between the government and the governed can be undermined by pervasive public video surveillance. Without procedural limits, law enforcement officers might use the technology to improperly surveil private activity or otherwise go beyond the bounds of their authority. Without accountability safeguards, the officers might never have to explain their actions.
- **Equal protection and anti-discrimination** rights, finally, are at risk. Discrimination, whether based on race, gender, religion, age, sexual orientation, socioeconomic status, or some other attribute, can occur during the development or use of public video surveillance

systems. For example, decisions about where the cameras will be placed can lead to a disproportionate impact on certain groups, or operators could improperly use the cameras to single out members of those groups.[65]

Further, as with economic cost, communities should assess whether alternative methods of achieving the same law enforcement objectives would significantly decrease the negative impact on constitutional rights and values. Aside from demonstrating support for constitutional rights and values, such analysis and careful planning can improve public acceptance of the system and deter lawsuits alleging violation of these rights.

6. Design the scope and capabilities of a public video surveillance system to minimize its negative impact on constitutional rights and values.

Those designing public surveillance systems should further limit the negative impact of video surveillance on their communities by limiting the duration, geographical coverage, and technological capabilities of the system. A public video surveillance system should have no greater scope or capabilities than reasonably necessary to achieve its purposes. A system so limited will minimize the negative impact on constitutional rights and values when the system is used properly, will help reduce the likelihood that the system will be abused or misused, and can avoid legal expenses that may otherwise be incurred defending the legality of the system.

A system may be limited in several respects. First, the duration that a system operates should be no longer than reasonably necessary to achieve its articulated purpose. As discussed in Section III.A.2., *supra*, the danger to constitutional rights and values increases with the duration of surveillance, and permanent systems should be created only to address threats to public safety that are of indefinite duration.

Second, a public video surveillance system should not cover more geographic territory than is reasonably necessary to achieve its purpose. For example, a temporary public video surveillance system created to combat criminal activities in a public park should be limited to the areas of the park in which the criminal activity occurs. More specifically, each camera should be placed or equipped in a manner that minimizes, where reasonable, its ability to surveil unnecessary areas, such as the windows of private residences.

Third, the cameras and the camera network should be equipped with only those features or capabilities reasonably necessary to serve the purpose of the system. Technological features like magnification, night vision, infrared detection, and automatic identification and tracking, which pose significant dangers to constitutional rights and liberties (*see* Section

II.A.2., *supra*), should be used only where they are needed. For instance, a camera network created to monitor a busy urban freeway for accidents or stopped vehicles likely does not require facial recognition technology—the use of which would increase the impact on civil liberties and increase the cost of the system without furthering its legitimate purposes of aiding motorists.

7. Create technological and administrative safeguards to reduce the potential for misuse and abuse of the system.

In addition to limiting the scope and capabilities of the system itself, communities should create a set of technological and administrative safeguards designed to deter, detect, and punish misuse and abuse of the public video surveillance system. These additional safeguards can further reduce the negative impact of the system on constitutional rights and values. Technological safeguards could include, for instance, employment of encryption technology (*see* Section II.A.2.e), *supra*) to help limit and control access to stored surveillance data. Similarly, administrative safeguards could include rules requiring archived surveillance data to be held by a government agency independent of law enforcement. The employment of such rules and technologies is addressed in Section C.

8. Ensure that the decision to create a public video surveillance system, as well as major decisions affecting its design, are made through an open and publicly accountable process.

Public oversight and accountability are a vital means of ensuring that any public video surveillance system is designed to prevent misuse and abuse. Members of the community that would be affected by a proposed system should have the opportunity to participate in the decision to create such a system, as well as the subsequent major decisions affecting its coverage and capabilities. Public input and oversight will force public officials seeking to deploy a surveillance system to justify the installation of cameras by demonstrating to the public that the anticipated costs and ill effect on constitutional rights and values are outweighed by the system's prospective benefits.

Although each community may adopt different processes depending on its unique needs and circumstances, any chosen procedure should preserve—at the least—some form of public accountability. We outline two recommended procedural mechanisms to evaluate public video surveillance systems in Section B.

B. Publicly Accountable Procedures for Establishing Public Video Surveillance Systems

This section outlines two recommended procedural means for creating and designing a public video surveillance system: (1) a detailed, participatory, and transparent process designed for permanent, large-scale public video surveillance systems that includes a "civil liberties impact assessment" and a cost-benefit analysis; and (2) a streamlined process involving judicial oversight and approval designed for shorter-term public video surveillance systems that must be implemented either quickly or in secret. While both procedures require law enforcement officials to justify their planned system according to the core principles outlined in Section A, the first is a public, deliberative process in which the community has input and authority. The second, in contrast, recognizes that such *ex ante* public input and review sometimes can undermine the valid purposes of public video surveillance. To nevertheless preserve openness and accountability to the extent possible, this second process allows judicial oversight to substitute for direct public participation.

There are numerous variations on these procedures that may better accommodate the needs of a specific community. Certain steps may be unnecessary, or additional steps may be added. Similarly, a mix of public deliberations and non-public judicial review may be appropriate. However, any chosen method should preserve some measure of oversight and informed analysis of the proposed system by a neutral and qualified decision-maker to determine if a proposed system's benefits outweigh its social and economic costs.

1. For permanent or long-term public video surveillance systems, conduct a civil liberties impact assessment and overall cost-benefit analysis.

Many communities will likely seek to create a permanent video surveillance system to combat threats viewed as severe and enduring (*see* Section III.A.2., *supra*).* For such systems, a community should engage in a "civil liberties impact assessment" ("CLIA") and cost-benefit analysis prior to deployment. The fundamental goal of this process is to verify in a public and accountable manner that the proposed system is a cost-effective and minimally invasive means of achieving its stated purposes.

* It should be noted that even if a camera installation is not explicitly deemed "permanent," if it persists for a long enough period of time it should be considered *de facto* permanent and subject to the requirements of a permanent system. For instance, if a temporary system deployed pursuant to the judicial authorization process (*see* Section III.B.2., *infra*) is repeatedly renewed, it should likely be considered "permanent" and therefore subjected to the procedures we recommend in this section.

This review process has several major steps, which may be repeated as necessary if analysis and debate lead to modifications in the proposal. These steps largely track the core principles outlined in Section A. While extensive, we imagine that this process will often help a community save money. The process will ease later installation, operation, and review of surveillance networks. Also, it can substantially reduce the risk that surveillance networks will become embroiled in costly litigation.

- **Articulation and evaluation of the legitimate law enforcement purposes that justify the system.** This requires answering basic questions such as whether authorities intend the system to deter and prevent harmful events, provide a means of investigating events after they occur, or both. Moreover, authorities should evaluate the overall "magnitude" of the threat by considering the impact of the harmful events, should they occur, and the likelihood of occurrence.

- **Production of an initial proposal outlining the geographic scope and capabilities of the system.** The proposal should provide as much detail as possible, including every location in which a camera is to be installed, the visual coverage of each camera, and the proposed technical specifications of the entire system.

- **Analysis of whether the proposed system will effectively address its purposes.** Proposed systems not likely to accomplish their intended goals should be abandoned or redesigned and resubmitted.

- **Analysis of the proposal's cost.** Authorities should consider all economic costs of the system—including equipment, installation, training, maintenance, operation, and oversight—as well as any economic benefits, such as increased tax revenues from businesses or improved real estate values.

- **Analysis of the impact of the system on constitutional rights and values (the CLIA).**[66] The CLIA must consider each camera location, its intended field of view and "incidentally" visible areas, and the capabilities of each camera and camera network. It should then study how the system will affect constitutional rights and values in each area to be surveilled, considering both the general character and current uses of these places.* The CLIA should also include any proposed technological or administrative safeguards that may mitigate the system's social impact. Authorities may want to pose the following questions:

* Different rights and values may be at stake to varying degrees depending on the nature of the place—for instance, free expression is likely a more primary consideration at a public park next to a city hall than an alleyway behind a shopping mall. Similarly, the deployment of identification technologies may significantly chill free expression in the park, but in the lobby of a government building, these technologies may have only a minimal effect on individuals already required to present identification.

- Will the surveillance be conducted in places where it is likely to infringe upon expectations of privacy and anonymity, such as outside restaurants, nightclubs, medical clinics, or political party offices?
- To what extent do the proposed cameras capture more detail and reveal more information than would be observed by a law enforcement officer at the scene?
- Are the places to be surveilled used for demonstrations, picketing, leafleting, or other activities protected by the First Amendment?
- Will the system create unaccountable law enforcement authority or unnecessarily increase the ability of negligent or rogue officers to misuse or abuse their authority?
- Is the surveillance likely to have a disproportionate impact on a minority group or marginalized portion of the population?

- **Overall cost-benefit analysis of the proposed system.** The overall cost of the system is a combination of its burden upon a community's resources and the adverse impact of the system upon the constitutional rights and values of individuals. The anticipated benefit of the system could be roughly conceptualized as the product of the magnitude of the threats and the expected efficacy of the system. If this analysis cannot demonstrate the positive value to the community of video surveillance, the proposal should either be abandoned or revised.

Fundamental to successful integration of a public video surveillance system into a community is maintenance of the people's right to be informed as to the design, scope, location, use, and misuse of the system (*see* Section II.B.3., *supra*). We believe that the major components of a *permanent* public video surveillance system should never be secret, as secrecy reduces the accountability of the authorities and prevents individuals from understanding the implications of their actions. (For discrete targeted criminal investigations requiring secrecy, law enforcement should use the judicial approval process outlined in Section III.B.2., *infra*.) The involvement of the public should thus be preserved through a variety of means:

- An elected or publicly accountable body, such as a city council, legislature, or county committee, should undertake this process.
- To the extent feasible, the deliberations and debate of this body should be open to the community, and should permit public commentary.
- The CLIA and cost-benefit analysis should culminate in a public draft report, with a period set aside for the public to submit comments.
- The process can be repeated as necessary: the government body should review the comments, make necessary changes, and resubmit a revised proposal, culminating in a revised report.

2. For temporary public video surveillance systems, demonstrate to a neutral magistrate that the system has no greater scope or capabilities than reasonably necessary to achieve a legitimate law enforcement purpose.

Recognizing that temporary public video surveillance systems often will require speedy deployment or secrecy, the public and deliberative nature of the CLIA and cost-benefit process described above may be impractical or even counter-productive. To preserve openness and accountability to the extent possible for such systems, however, we propose a streamlined process that substitutes judicial oversight for full public participation. This process also reflects the fact that temporary systems inherently pose less threat to constitutional rights and values than permanent systems, all else being equal (*see* Section III.A.2., *supra*). Like the corresponding public process, the judicial approval process requires law enforcement to justify the planned system according to the core principles outlined in Section A.

In order to obtain judicial approval through this process, law enforcement must first show that the proposed system both (a) will be temporary and (b) requires speed or secrecy* to be effective. Should law enforcement be unable to make this showing, the system merits a full, public process, and the reviewing court should dismiss the proposal. Once this first hurdle is cleared, law enforcement must then demonstrate that the system has no greater scope or capabilities than reasonably necessary to achieve a legitimate law enforcement purpose. The steps required to make this showing are a streamlined version of the steps outlined in the previous guideline: [67]

- Explain the legitimate law enforcement purposes of the proposed system and show that the installation of surveillance cameras will produce evidence useful in serving these purposes.
- Show that the planned surveillance is likely to be more effective than other reasonable means of investigating or combating the crimes at issue.
- Describe the places and activities to be surveilled, and explain why surveillance of those locations and activities is reasonably necessary to further the law enforcement objectives.
- Demonstrate that the technological scope of the proposed system is not more powerful than reasonably necessary to further the law enforcement objectives.
- Demonstrate that the video surveillance will be limited to a period of time no longer than reasonably necessary to achieve the stated objectives.

* While the court proceedings would generally be public, those aspects of the system requiring secrecy could be presented *in camera* or pursuant to a confidentiality order.

- Show that the system contains other protections and safeguards to minimize the intrusion into the constitutional rights and values of individuals whose images will be captured by the surveillance but who are not suspected of criminal activity.

Finally, after law enforcement has demonstrated the above to the satisfaction of the magistrate, the system should be approved for the specified time period. Extensions should require further review and approval.

C. Principles and Rules for Use of Public Video Surveillance Systems

This section discusses rules and procedures designed to ensure that a system, once installed, is used in accordance with core substantive principles. It describes the different functions which video surveillance systems may perform—observation, recording, tracking, and identification—and outlines rules governing each type of use, with progressively tighter control recommended for each. (The technologies associated with these various types of video surveillance are described in Section II.A.2., *supra*.) It further describes technical and administrative constraints on the use of surveillance systems, including secondary uses of information gathered through surveillance, the retention of stored surveillance data, and the rights of identifiable individuals captured on camera.

1. Once a public video surveillance system is authorized, no additional approval is necessary to use the capabilities of the system for "observation."

In the context of public video surveillance systems, we define "observation" as real-time viewing of live camera images. In the case of pure observation, no permanent record of an individual's activities, other than the operator's memory, will persist once the image is replaced with a new one. Relative to the other law enforcement uses of the system, observation is perhaps closest to the familiar, low-tech visual surveillance to which individuals are already accustomed. For this reason, observation generally presents the smallest risk of infringement of constitutional rights and values. Moreover, so long as a community has agreed to adopt video surveillance based on the procedures described in Section B above, *ex ante* restriction of simple observation adds little protection, since camera monitors cannot know what they will see until they see it. It is thus impractical and unnecessary to require advance approval before using permanent video camera installations for observation. Law enforcement officers observing public places through a video surveillance system should be able to act upon the information gathered as if they had witnessed it at the scene.

It is true that observation can pose significant dangers to constitutional rights and values. For example, the selection of which cameras to observe can be racially or otherwise biased and lead to discriminatory use of the resulting evidence. Moreover, technological supplements can significantly change the system's capabilities. As described in Section II.A.2.a), *supra*, magnification can reveal significantly more detail than would be visible to a human observer, and low-light or infrared cameras can see in darkness far better than the human eye. Based on the infringement of constitutional rights and values possible with such technology, these features should be carefully considered during the system's design approval phase. Moreover, the use of these technologies should be closely evaluated during the audit and review process, and law enforcement should create internal procedures to regulate how such capabilities may be used (*see* Section III.C.5.b), *infra*). Once the system has been approved, however, no additional *ex ante* approval is needed to use observation technologies.

2. "Record" footage from public video surveillance systems only to the extent necessary to further the system's stated purposes.

More significant in its implications is "recording," where images are preserved and stored for later review. Nearly unlimited amounts of recorded digital footage may be cheaply stored in databases, which may then be supplemented with metadata and quickly retrieved on demand (*see* Section II.A.2.b), *supra*). The stored data poses the risk that it will later be misused, lost, stolen, or repurposed—all of which undermine constitutional rights and values.

As with observation, however, the rules regulating the recording of video data should be established at the design phase of the system. General rules should govern if and when data should be recorded, and for how long it should be stored. A community may decide that a given camera or network should always record, record on request, record automatically in certain situations, or never record. These rules should ensure that the system records and stores video footage only to the extent necessary to further the system's stated purposes. More specific *ex ante* approval for recording would be neither practical nor useful.

Recorded footage lacking evidentiary or other documented value should be destroyed as a matter of course after a specified time. Any decision to retain footage past the time period allotted in the policy should be specifically documented for subsequent review and audit. All saved footage, regardless of age, should be closely monitored and protected—by procedural and/or technological means (*see* Section III.C.5., *infra*). Unlike the *recording* of video footage, *access* to stored footage will require *ex ante* approval in many cases (*see* Section III.C.4., *infra*).

3. Under most circumstances, individuals may be "tracked" or "identified" by a public video surveillance system only pursuant to a warrant.

Most dangerous to constitutional rights and values is the ability of modern camera networks to "identify" and "track" individuals, and thus additional precautions are required. "Tracking" refers to the use of public video surveillance systems to automatically follow an individual or her vehicle, regardless of whether her identity is known, so as to create a seamless record of her activity during a specific period.* "Identification" refers to the use of the system to ascertain or confirm the identity of an individual captured on video footage.† Tracking and identification can occur in real time or by using stored video footage. Although an individual may be identified without being tracked, or vice versa, we discuss the two terms together—distinguishing one from the other where necessary—since they raise similar concerns. See Section II.A.2., *supra*, for a discussion of tracking and identification technologies.

The use of identification and tracking technologies raises specialized concerns regarding constitutional rights and values. Even in public, most people expect to remain anonymous unless they are seen, recognized, and remembered by another individual present in that location. Pervasive use of automated identification undermines this expectation—implicating privacy, anonymity, and First Amendment freedoms. Even tracking alone can create a far more thorough record of activity than observation and recording. Identification, moreover, creates a record that is personally identifiable and traceable back to a specific person, which raises data privacy concerns far less present with other types of surveillance.[68] Finally, identification systems raise the potential for troubling issues of discriminatory profiling and misidentification. These concerns justify more stringent restrictions than necessary for other video surveillance technologies.

* The limitations in this section do not apply law enforcement's ability to *manually* track an individual within a camera view (using pan and tilt functions) or between separate cameras by manual means.

† Identification includes manually appending personally identifiable information, such as name, address, or criminal history, to recorded images of those individuals, or automatically identifying an individual captured on video footage, in real time or using stored data, using biometric or other identification algorithms. These guidelines do not attempt to place specific limitations on identification of individuals in video footage based on visual recognition by law enforcement personnel or other individuals. Should that identification be entered into a database for later searching, however, the identification would be considered automatic and within the scope of this guideline.

a) Law enforcement must obtain a warrant prior to using a public video surveillance system to track or identify an individual.

Subject to the traditional constitutional law exceptions and the use of federal anti-terrorism watch lists (discussed below), we recommend that law enforcement must obtain a warrant—limited as to the scope of the investigation—in order to use a public video surveillance system to identify or track an individual. Though, under current constitutional jurisprudence, a warrant is generally not required for use of public video surveillance (*see* Section II.C.1., *supra*), we recommend application of similar standards and procedures to those required for a search warrant under the Fourth Amendment. In other words, law enforcement officers must demonstrate to a neutral magistrate that they have probable cause to believe that tracking or identifying a specific individual through use of a public video surveillance system will reasonably lead to the discovery of specified evidence of wrongdoing.[69] As with search warrants in the constitutional context, some narrow exceptions would apply—such as when the individual has consented to the identification or tracking or when exigent threats to public safety require action before judicial approval can be obtained.

As with warrant requirements in the context of other electronic surveillance, use of this procedure is likely to save resources that law enforcement would otherwise be forced to employ defending against legal challenge to surveillance evidence.

b) Law enforcement must obtain a warrant prior to using a "watch list" to automatically identify individuals, except when using a federal anti-terrorism watch list.

Watch lists are precompiled lists of suspects and persons of interest used by the government for various law enforcement or national security purposes. For example, law enforcement might wish to create a watch list of the biometric profiles of individuals who are persons of interest in a criminal investigation, and then program certain video cameras to scan for biometric matches in case those individuals enter the surveilled area. Use of watch lists in conjunction with video surveillance increases the risk to constitutional rights and values, since they require constant use of identification technologies in the surveilled area to be effective. They also raise additional concerns about "false positive" matches that can lead to mistreatment of innocent individuals.

In general, we recommend that law enforcement must obtain a warrant to create a watch list or add individuals to an existing list. Specifically, officials should demonstrate to a neutral magistrate that they have probable cause to believe that identification of the specific individual will lead to evidence helpful to a particular criminal investigation. If law

enforcement officers obtain an arrest warrant for an individual, the showing required for the arrest warrant should suffice for addition of the individual to a watch list.

However, we recommend creating an exception for the use of anti-terrorism watch lists compiled by the federal government, because the reliability and necessity of federal anti-terrorism watch lists must be presumed.* This recommendation is based upon the national security and secrecy concerns underlying the federal lists as well as the practical concern that local officials likely would not be permitted access to the underlying data they would need to justify a warrant in court. This exception does not apply to any other watch lists, regardless of source.

4. A public video surveillance system may be used for legitimate law enforcement purposes other than its original purpose, subject to certain restrictions.

Although not all law enforcement purposes will justify creation of a public video surveillance system, once a system has been properly designed and implemented pursuant to a publicly accountable procedure, it may collect data that would be relevant to other legitimate law enforcement uses. Subject to certain restrictions (discussed below), law enforcement may use the system for these new purposes. Because the scope and capabilities of the system remain unchanged, new uses for the system should not pose significantly greater threats to constitutional rights and values than existing ones.

We distinguish between two types of extra-purpose use of video surveillance data and systems—"secondary" and "incidental." Secondary use is an intentional, planned use of a system, a component of it, or the collected data, for a purpose other than the original one. For instance, if an officer has reason to believe that stored footage collected for traffic control purposes would show evidence of drug shipments and seeks to review the footage for this purpose, the use would be secondary. In contrast, incidental use describes a situation in which law enforcement is using the system for its intended purpose and incidentally notices something useful for a different purpose. For instance, if an officer monitoring a surveillance system deployed to prevent a terrorist attack incidentally witnesses a non-terrorism crime, the information would be useful for the purpose of investigating that crime.

* Although we have concerns regarding federal anti-terrorism watch lists, including the processes by which they are compiled, these concerns are beyond the scope of this report.

a) No additional approval is required for incidental use of the system.

A public video surveillance system properly installed in a publicly accountable fashion may be used incidentally for other legitimate law enforcement purposes. Similar to the "plain view" exception in Fourth Amendment law,[70] a police officer properly observing public scenes through a visual surveillance system should be able to act upon evidence of criminal behavior as if she had witnessed it in person. This is true whether the officer is viewing the footage in real time or via a recording.

b) Law enforcement must obtain administrative approval for secondary use of "pre-archival" stored video surveillance footage.

For regulation of secondary uses, we further distinguish between "pre-archival" and "archival" storage of video surveillance footage. "Pre-archival" footage is recently recorded data subject to routine review by law enforcement. This category may extend to include a community that, rather than staffing officers to observe every camera in real time, reviews recorded footage on a daily or weekly basis. "Archival" footage is data that has been stored beyond the short time period designated for routine review. A locality can define a reasonable time frame within which law enforcement must complete its routine review, after which the footage becomes "archival." This distinction should be based on actual law enforcement practices rather than an artificial label.

Law enforcement may use pre-archival video footage for a secondary purpose if it secures administrative approval. No judicial approval is required, though the process and substantive standard for approval should be similar to the warrant process. That is, law enforcement officers should demonstrate that they have probable cause to believe the footage will provide evidence of specific criminal acts. The administrator may be an official in the law enforcement organization itself, but the approval process should be recorded and reported to the public for subsequent review and audit.

c) Law enforcement must obtain a warrant for secondary use of "archival" stored video surveillance footage.

Law enforcement may use archived video footage for a secondary purpose only if it secures a warrant from a neutral magistrate, as per the procedure described above (*see* Section III. C.3.a), *supra*). Such a rule preserves greater protection of archived footage, which may be voluminous. Nor do we expect such a requirement to be too great a burden: by the time footage is archived, there will rarely exist a secondary purpose that requires review so quickly that judicial approval cannot first be obtained.

5. Employ technological and administrative safeguards to reduce the potential for misuse and abuse of the system.

Technological and administrative safeguards are an important component of any public surveillance system. They should generally be developed at the design stage for the system (*see* Section III.A.7., *supra*).

a) Provide safeguards for use of stored video surveillance data.

The ability of a system to store video surveillance data can be technologically limited (*see* Section II.A.2.e), *supra*, for more information). For instance, a system intended for observation alone could be technologically prevented from recording at all. Similarly, a system designed to monitor traffic can automatically delete its data the following day. Administrative limits can have a similar effect, or be used in conjunction with limiting technologies. For many public video surveillance systems, however, some data will have ongoing value and must be stored for a long or indefinite period. For such storage, communities may employ specific safeguards:

- Encryption technology can prevent those without the proper decryption keys from having access to the stored data. Encryption is inexpensive, and can eliminate virtually any possibility that lost or stolen data will be misused.
- Use of "digital masking" or other technologies to remove identifying features of individuals who are incidentally captured on camera or whose identities are otherwise irrelevant to the purposes for which the data is stored. Photo-enforced traffic law systems already make use of similar technology by blurring the faces of passengers in issued citations.
- Administrative rules, used in conjunction with encryption, can require that stored footage be entrusted to a neutral entity, such as a public auditor independent of law enforcement. This entity can review requests for access to the stored data based on established procedures, and surrender access only when law enforcement can demonstrate a sufficient need for specified footage. If the data is encrypted, such an entity need not physically store or control the data; it can simply hold the encryption keys and access logs for the data.
- The use of digital watermarks or similar technologies can help create a clear record of when and where records were accessed. Administrative rules can similarly require officers to log when, where, and why they access stored footage.
- Data security technologies can be employed to protect the integrity of the data from hacking or other risks.

- Access to stored data can be limited to authorized personnel or individuals with a demonstrated interest in the footage (i.e., to defend themselves against a criminal charge).

b) Provide safeguards for personnel with access to a public video surveillance system.

Personnel who operate or have access to a public video surveillance system are obviously those who pose the greatest risk of abuse or misuse of the system. They should therefore be subject to various safeguards:

- Physical access to the facilities—such as control rooms, databases, or cameras—should be limited to authorized and screened personnel.
- All personnel authorized to have such access should undergo a training program covering both the technical operation of and applicable laws and rules regarding the system, including a discussion of sanctions for misuse or abuse.
- Administrative rules should govern when operators may use various system capabilities. For instance, to protect against discriminatory or arbitrary application, operators should use zoom or manual pan and tilt features pursuant to established "triggering" events and situations.
- Personnel failing to comply with rules regulating the operation of a video surveillance system should face sanctions, including reprimands, fines, and criminal penalties.

c) Provide public notice of surveillance where appropriate.

To permit informed choices and provide accountability, those subject to video surveillance should be made aware of it. While many communities will want to hide or disguise the actual cameras for security as well as aesthetic and social reasons, there is generally no basis for hiding the fact that an area is under government surveillance. These notifications need not be intrusive, but should nevertheless be visible. We recommend that authorities place small placards in the surveilled area noting the presence of video surveillance and providing contact information for those wishing more information about the camera system. Such placards may in fact increase a system's deterrent effect.

Permanent public video surveillance systems should never be installed in secret (*see* Section III.B.1., *supra*), nor should the general locations of permanent cameras be withheld from the public. Permanent systems, therefore, should always include the type of notice discussed above. Some temporary systems may require secrecy. Should law enforcement wish to keep the fact or location of temporary video surveillance secret, permission must be obtained from a magistrate as part of the judicial approval process (*see* Section III.B.2., *supra*).

6. Prohibit, to the extent possible, sharing of public video surveillance data with third parties, including private litigants, and restrict sharing with other governmental entities.

Communities should restrict use of public video surveillance data by third parties. Especially to the extent the data reveals identifiable individuals, sharing of data with private litigants or other governmental agencies without the consent of the affected individuals severely undermines confidence in official motives for collecting such information, further threatens constitutional rights and values, and could generate legal liability for law enforcement. While releasing footage may be beneficial in some cases, such as to enlist public aid in apprehending a suspect or to perform an audit, in general, disclosures to third parties creates increased risk of the information being used for improper and unaccountable purposes.

Data collected by public video surveillance systems should generally not be available, or in any way discoverable, in a civil trial between private litigants. Private litigants would no doubt appreciate access to this data—not only in divorce cases, but also in traffic accidents, workers compensation claims, and a host of other cases. Such widespread use, however, would further infringe upon constitutional rights and values for private benefit. Private litigants, journalists, and others may also seek to employ the Freedom of Information Act (*see* Section II.C.2., *supra*) to obtain surveillance records. In addition to the implications for the rights and liberties of those captured on the requested footage, compliance with such requests can be extremely expensive if records are voluminous. While the privacy exception to FOIA may permit authorities to deny such requests, it is unclear how courts will interpret FOIA in this regard. Authorities can avoid much of this expense and danger to constitutional rights and values by destroying archived records as soon as possible.

Limitations should also apply, to the extent possible, to inter-governmental sharing of public video surveillance data. Authorities who are not accountable to the residents of the original jurisdiction may not adequately protect the surveillance footage of those residents. Other governmental authorities seeking access to the data should apply for a warrant from a neutral magistrate to demonstrate their need for the data in accordance with the standard in Section III.C.3.a), *supra*. However, some inter-government sharing must be allowed without a warrant. To the extent that federal law, for instance, requires sharing with federal law enforcement, local officials are of course bound to comply. Nevertheless, such required sharing should be disclosed to the public and the affected individuals whenever possible.

7. Establish mechanisms to protect the rights of identifiable individuals captured on video surveillance data.

Whether accomplished through biometric identification technologies or manual data entry, public video surveillance records can become personally identifiable information when an otherwise anonymous image is linked to a specific, identified person. Communities should establish rules requiring that whenever such data is collected or stored, the individuals so identified possess additional rights to help protect against the greater threats to constitutional rights and values posed by such records.

As a preliminary matter, law enforcement should protect individuals' privacy by avoiding unnecessary identification of particular people. Specifically, when law enforcement uses recorded footage, techniques such as "digital masking" (*see* Section II.A.2.e), *supra*) should be employed where feasible to automatically hide the faces of individuals who are not the subject of the investigation. Note that a community can eliminate much of any burden created by such necessary protections by using technology to ensure that unneeded identifying information is not stored at all.

Further, individuals should be protected through additional rights that generally track the substance of the Fair Information Practices (*see* Section II.C.2., *supra*).

- **Notice and awareness.** The community should be notified if and how the system collects, possesses, or uses personally identifiable video surveillance information (*see* Section III. C.5.c), *supra*).
- **Consent.** Where feasible, use or sharing of personally identifiable video surveillance information outside of the system's original purposes should occur only with the consent of the individual. For instance, should law enforcement wish to publish surveillance footage of a violent attack in order to enlist public help in locating the attacker, it should obtain the consent of the victim, if the footage identifies him, or rely on masking techniques to avoid such an identification.
- **Access and participation.** Unless valid law enforcement reasons prohibit it, individuals should have the right to request a report of their identified appearances—namely images that have been labeled or tagged with a person's name and/or other identifying information—on surveillance footage. Furthermore, individuals should have a reasonable opportunity to amend their data if it contains errors or inaccuracies.
- **Integrity and security.** Authorities in control of personally identifiable video surveillance information must take reasonable precautions to keep it secure (*see* Section III.C.5.a), *supra*).

8. Apply to any law enforcement use of privately collected video surveillance data the same standards that apply to public video surveillance data.

Private parties generate a substantial amount of surveillance footage, some of which becomes valuable to law enforcement. Footage from ATM cameras, for instance, captured images of some of the September 11th hijackers. Should law enforcement obtain such footage, it should follow all applicable rules discussed in Section III.C. Thus, use of the data to track or identify individuals should only be accomplished pursuant to a warrant, subject to the usual warrant exceptions; all technological and administrative safeguards applicable to public video surveillance data should be applied; personnel with access to such data should be trained; and any personally identifiable video surveillance information should be afforded additional protection.

9. Provide appropriate remedies for those harmed by misuse or abuse of public video surveillance systems.

Even a carefully designed and limited public video surveillance system can injure innocent individuals. Use of biometric profiles to identify an image of an individual can generate a "false positive," a bored operator can become a voyeur, or an impatient officer can obtain stored data without a warrant. In these instances, those injured should have redress. The following is a sample of potential remedies, which may be appropriate for different types of violations.

- **Exclusion of evidence.** In the criminal context, exclusion of improperly obtained evidence provides both a remedy to the injured criminal defendant and a powerful deterrent to law enforcement.[71] We recommend that states require that public video surveillance data collected in a major violation of the system's rules would similarly be excluded (e.g., an officer fails to obtain a necessary warrant, or a system identifies the defendant using biometric identification software that was never approved by the community).
- **Private rights of action.** Injured parties could also be provided with a private right of action to bring suit for redress.
  - **Injunctive relief.** To provide a deterrent or to punish misuse or abuse, a community could allow injured parties to seek to enjoin uses of a public video surveillance system that fail to comply with the system's stated purposes or limits.
  - **Monetary damages.** The community could require the government to compensate those harmed by the system. While damages calculations are difficult in the privacy and civil liberties context,[72] statutory damages or class action suits could ensure that the awards are sufficient to remedy harms and deter bad behavior.[73]

- **Informal remedies.** In addition to using the courts, the law enforcement agency itself can provide less formal remedies, such as issuance of public corrections or apologies for mistakes or misuse.

IV. Conclusion

The emergence of powerful video surveillance technologies is already providing law enforcement with invaluable new tools for battling crime and terrorism. As would-be criminals and terrorists themselves gain access to powerful new weapons and technologies, American law enforcement should likewise be able to take advantage of technological developments to protect the lives and safety of innocent individuals. However, these technologies must be designed and used not only to protect Americans against crime and terrorism, but also in ways that preserve accountability, procedural safeguards, and constitutionally protected rights of privacy, freedom of expression, and freedom of association. Public camera systems arrayed over public spaces might not only deter criminals or terrorists from attacking, but could also intimidate individuals who express opposition to government positions, deter speech or associations considered eccentric or unpopular, or undercut the insulation that Americans have traditionally enjoyed against pervasive government monitoring of their personal affairs.

For this reason, the Constitution Project's Liberty and Security Initiative encourages lawmakers at all levels of government to think carefully about the permissible design and use of these potentially dangerous new surveillance technologies. We intend the principles we have outlined and described here to guide this inquiry. We hope that the Constitution Project's *Guidelines for Public Video Surveillance* provide a useful framework for protecting core constitutional freedoms and social values in a world of technologically-assisted law enforcement and real, serious threats to public safety.

Finally, to further assist communities to reconcile law enforcement goals with constitutional rights and values, the Constitution Project, in conjunction with the Samuelson Law, Technology & Public Policy Clinic at U.C. Berkeley's Boalt Hall School of Law, has developed model legislation designed to codify these guidelines. We hope that communities considering implementation of public video surveillance systems will be able to use this model legislation when establishing such systems in their own jurisdictions.

ENDNOTES

1 Quentin Burrows, *Scowl Because You're on Candid Camera: Privacy and Video Surveillance*, 31 Val. U.L. Rev. 1079, 1103 (1997). For a discussion of the history of video surveillance, *see* Robert D. Bickel, Susan Brinkley & Wendy White, *Seeing Past Privacy: Will the Development and Application of CCTV and Other Video Security Technology Compromise an Essential Constitutional Right in a Democracy, or Will the Courts Strike a Proper Balance?*, 33 Stetson L. Rev. 299, 301–07 (2003).

2 Eric Weiss, *D.C. Considering More Police Cameras*, Wash. Post, July 14, 2005, at B1 (citing the usefulness of video footage in the 2005 London bombing investigations in recent discussions of expanded surveillance systems).

3 *Cameras may yield clues to London attacks*, MSNBC, July 7, 2005, http://www.msnbc.msn.com/id/8501576/.

4 *See* Christopher Slobogin, *Public Policy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 Miss. L.J. 213, 222 (2002).

5 Steven Kinzer, *Chicago Moving to 'Smart' Surveillance Cameras*, N.Y. Times, Sept. 21, 2004, at A18.

6 *See generally* Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. Cal. L. Rev. 1083 (2002); Daniel J. Solove, The Digital Person: Technology and Privacy in the Information Age (2004).

7 Google Earth: A 3-D interface to the planet, http://earth.google.com/.

8 *See* Ed Frauenheim, *Computer system said to help stop drowning*, CNET News.com, Jan. 31, 2005, http://news.com.com/Computer+system+said+to+help+stop+drowning/2100-1041_3-5558015.html (reporting on a camera by Poseidon Systems described at Poseidon, The Lifeguard's Third Eye, http://www.poseidon-tech.com/us/index.html).

9 This, for example, is how a murderer was identified in Florida in 2003. *Housemate Tips Police to Smith After Seeing Video*, CNN.com, Feb. 6, 2004, http://www.cnn.com/2004/US/South/02/05/missing.girl/index.html.

10 *See* Mary Jordan, *Electronic Eye Grows Wider in Britain*, Wash. Post, Jan. 7, 2006, at A1, *available* at http://www.washingtonpost.com/wp-dyn/content/article/2006/01/06/AR2006010602100.html.

11 As one scholar noted, polls regarding devices like the E-ZPass automated toll system show that even when the information is "not very personal or private," people nonetheless "seem to be concerned when a comprehensive information profile is constructed about *any* aspect of their lives." Dorothy J. Glancy, *Privacy and Intelligent Transportation Technology*, 11 Santa Clara Computer & High Tech. L.J. 151, 165 (1995) (emphasis added).

12 *Cf.* Noah Shachtman, *The New Security: Cameras That Never Forget Your Face*, N.Y. Times, Jan. 25, 2006, http://www.nytimes.com/2006/01/25/technology/techspecial2/25video.html ("For now—and the foreseeable future—[commercial facial recognition software] is effective only in small, controlled environments where the lighting is consistent and only a few people pass in front of one camera at a time. Picking out criminal suspects on the street or in a crowd—as the city of Tampa, Fla., tried to do in its Ybor City district from 2001 to 2003—is still beyond the ability of [commercially available] surveillance system[s].").

13 *See* Paul Festa, *Face recognition gets lift, U.S. says*, CNET News.com, Mar. 25, 2003, http://news.zdnet.com/2100-1009_22-944111.html.

[14] *See* Fred Guterl & William Underhill, *Taking A Closer Look*, Newsweek, Mar. 8, 2004, at 42. According to local authorities however, Virginia Beach recently ceased operation of its facial recognition technology due to its ineffectiveness.

[15] *Morning Edition: Profile: Use of Surveillance Cameras in New York City and Other Places Around the World* (NPR radio broadcast Feb. 25, 2002) (noting reports of thousands of cameras in New York City and deliberations about installing "a hundred cameras with face recognition software in Times Square").

[16] John D. Woodward, Jr., *Case Study: Super Bowl Surveillance, in* John D. Woodward et al., Biometrics: Identity Assurance in the Information Age 247, 251 (McGraw-Hill 2003).

[17] *See, e.g.,* Elaine Newton, et al., *Preserving Privacy by De-identifying Facial Images*, Carnegie Mellon Univ., Sch. of Computer Sci., Technical Report No. CMU-CS-03-119, Mar. 2003, *available at* http://privacy.cs.cmu.edu/people/sweeney/CMU-CS-03-119-600dpi.pdf (proposing a mechanism by which "face recognition software is restricted" but details allowing for comparison between different anonymous images remain, so that "society can have both safety and privacy").

[18] *See, e.g.,* Jess Bravin, *Washington Police to Play 'I Spy,'* Wall St. J., Feb. 13, 2002, at B1 (reporting that Washington, D.C.'s cameras "already monitor mass-transit stations, monuments, and schools" and that officials have announced plans to extend the monitoring to "streets, shopping areas, and neighborhoods," creating "one of the nation's most extensive public surveillance networks").

[19] Kinzer, *supra* note 5.

[20] Hal Dardick, *City Will Keep Eyes Peeled Big Time*, Chi. Trib., Feb. 11, 2005.

[21] *Id.*

[22] David A. Fahrenthold, *Federal Grants Bring Surveillance Cameras to Small Towns*, Wash. Post, Jan. 19, 2006, at A1, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2006/01/18/AR2006011802324.html (describing how local law enforcement officers, due to the limits imposed on the use of federal anti-terrorism funding, are increasing their use of video surveillance). *See also* Electronic Privacy Information Center, Spotlight on Surveillance: *More Cities Deploy Camera Surveillance Systems with Federal Grant Money* (May 2005), http://www.epic.org/privacy/surveillance/spotlight/0505/.

[23] Stephen Greenhalgh, *Literature Review on Issues of Privacy and Surveillance Affecting Social Behaviour* (Aug. 2003), http://www.oipc.ab.ca/ims/client/upload/LitReview.pdf (written for the Office of the Information and Privacy Commissioner of Alberta).

[24] *Id.* at 1.

[25] *Privacy vs. Security: Electronic Surveillance in the Nation's Capital: Hearing Before the Subcomm. on D.C. of the House Comm. on Gov't Reform,* 107th Cong. (2002) (statement of Johnny Barnes, Executive Director, American Civil Liberties Union of the National Capital Area).

[26] *Id.*

[27] *Olmstead v. United States,* 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting). *See also* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy,* 4 Harv. L. Rev. 193, 205 (1890).

[28] Alan F. Westin, Privacy and Freedom 31 (New York: Athenaeum 1967). *See also* Slobogin, *supra* note 4.

[29] Westin, *supra* note 28, at 31.

[30] For example, the Supreme Court has recognized that political or religious expression is not "free" if speakers are obliged to disclose their identity. *See McIntyre v. Ohio Elections Commission,* 514 U.S. 334, 343 (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 political causes") (citing *Talley v. California,* 362 U.S. 60 (1960)); *Watchtower Bible & Tract Soc'y of N.Y., Inc. v. Village of Stratton,* 536 U.S. 150, 166–69 (2002) (declaring unconstitutional a town law requiring those who wish to canvass door-to-door to first identify themselves in a permit application filed with the mayor's office and made available for public inspection). Similar rules apply to free expression rights, *see Lamont v. Postmaster General,* 381 U.S. 301 (1965) (striking down government measure that required individual to notify post office of interest in certain political materials before receiving them in mail), and freedom of association. *See NAACP v. Alabama,* 357 U.S. 449, 462 (1958) (forbidding the state of Alabama from compelling the NAACP to disclose its membership lists).

[31] *See* William H. Rehnquist, *Is An Expanded Right of Privacy Consistent with Fair and Effective Law Enforcement? Or: Privacy, You've Come a Long Way, Baby,* 23 Kan. L. Rev. 1, 9 (1974) ("Suppose that the local police in a particular jurisdiction were to decide to station a police car at the entrance to the parking lot of a well-patronized bar from 5:30 p.m. to 7:30 p.m. every business day for the purpose of making a list of the license plates of cars that were driven in and parked in the lot during that time… I would guess that the great majority of people who might have the question posed to them would say that this is not a proper police function… There would be an uneasiness, and I think a justified uneasiness, if those who patronized the bar felt that their names were being taken down and filed for future reference.")

[32] For instance, the U.S. General Accounting Office noted in assessing the constitutionality of Washington, D.C.'s new public video surveillance system that there is no Fourth Amendment concern raised by video cameras used only in public space. GAO, Report to the Chairman, Comm. On Government Reform, House of Representatives, *Video Surveillance: Information on Law Enforcement's Use of Closed Circuit Television to Monitor Selected Federal Property in Washington D.C.* (June 2003).

[33] *See Lamont v. Postmaster General,* 381 U.S. 301, 303 (1965) (invalidating a Federal law requiring recipients of "communist political propaganda" to specifically authorize the delivery of each such piece of mail).

[34] *See Watchtower Bible & Tract Soc'y of N.Y., Inc. v. Village of Stratton,* 536 U.S. 150 (2002) (expression); *NAACP v. Alabama,* 357 U.S. 449 (1958) (association).

[35] *See* Slobogin, *supra* note 4, at 257.

[36] 304 U.S. 144, 153 n.4 (1938).

[37] Brandon C. Welsh & David P. Farrington, Home Office Research, Development and Statistics Directorate, *Crime prevention effects of closed circuit television: a systematic review,* Home Office Research Study 252 (Aug. 2002), http://www.homeoffice.gov.uk/rds/pdfs2/hors252.pdf.

[38] *See* Jeffrey Rosen, *A Watchful State,* N.Y. Times Mag., Oct. 7, 2001, at 38.

[39] Avis Thomas-Lester & Toni Locy, *Complaint of Extortion Attempt Led to Probe of Police Unit,* Wash. Post, Nov. 12, 1997, at B4.

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

[41] *Dow Chemical Co. v. United States,* 476 U.S. 227, 238–39 & n.5 (1986).

[42] *See, e.g., Rodriguez v. United States,* 878 F. Supp. 20, 24 (S.D.N.Y. 1995) (finding no expectation of privacy in public street); *McCray v. State,* 84 Md. App. 513, 519 (1990) (finding no expectation of privacy where complainant filmed walking across a public street). Some courts have found the Fourth Amendment implicated in surveillance of private places—even those visible from public vantage points. *See United States v. Torres,* 751 F.2d 875 (7th Cir. 1984) (Posner, J.). In scholarly journals, many have argued that the Fourth Amendment is properly read to include restrictions on public video surveillance, but their arguments remain theoretical. *See, e.g.,* Marc Blitz, *Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World that Tracks Image and Identity,* 82 Tex. L. Rev. 1349 (2004); Slobogin, *supra* note 4, at 257.

[43] *See, e.g., Hague v. CIO,* 307 U.S. 496, 515 (1939) (Roberts, J., concurring) ("Wherever the title of streets and parks may rest, they 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 thoughts 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.").

[44] *See, e.g., Minneapolis Star & Trib. Co. v. Minnesota Comm'r of Rev.,* 460 U.S. 575 (1983) (holding that a tax on large quantities of ink and newsprint was unconstitutional because it burdened newspapers disproportionately).

[45] *See* Slobogin, *supra* note 4, at 253.

[46] *Laird v. Tatum,* 408 U.S. 1 (1972).

[47] 18 U.S.C. §§ 2510–2520. The statute defines a "wire communication" as "any aural transfer made . . . through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception." 18 U.S.C. § 2510(1).

[48] *See Kee v. City of Rowlett,* 247 F.3d 206 (5th Cir. 2001).

[49] USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001) (modifying 50 U.S.C. § 1861 to allow use of secret orders for the production of records related to terrorism investigations); FISA, 50 U.S.C. §§ 1801 et. seq.

[50] Freedom of Information Act, 5 U.S.C § 552(b)(7) (excluding from FOIA "records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information . . . could reasonably be expected to constitute an unwarranted invasion of personal privacy").

[51] *See* U.S. Dep't. of Health, Education and Welfare, *Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems* (1973).

[52] Council Directive 95/46, art. 8, 1995 O.J. (L 281) 31 (EC). These guidelines use the Fair Information Practices to support a framework for treatment of video data containing information about identifiable individuals. *See* Section III.C.7., *infra*.

[53] *See* N.Y. Crim. Proc. Law, Ch. 11-A, Pt. 3, Title T ("Procedures for Securing Evidence by Means of Court Order and for Suppressing Evidence Unlawfully or Improperly Obtained"), Art. 700. *See also* N.Y. Crim. Proc. Law § 700.20 (2002). The law includes serious felonies and drug-related crimes as sufficient to merit video surveillance. *Id.*

[54] Ariz. Rev. Stat. § 13-3019 (2001).

[55] *See* ABA Standards for Criminal Justice, Electronic Surveillance, Section B: Technologically-Assisted Physical Surveillance (3d ed. 1999), at 2.

[56] *See id.,* Standard 2-9.1(a) ("Technologically-assisted physical surveillance can be an important law enforcement tool. It can facilitate the detection, investigation, prevention and deterrence of crime, the safety of citizens and officers, the apprehension and prosecution of criminals, and the protection of the innocent.").

[57] *See id.,* Standard 2-9.1(b).

[58] *Id.,* Standard 2-9.1(c), Commentary to Standard 2-9.1(c) (at 28).

[59] *See, e.g., id.,* Standard 2-9.1(f) (on "Accountability and Control") and 2-9.3(b)(i) (under which use of overt public video surveillance must be authorized to meet certain standards by "a politically accountable law enforcement official or the relevant politically accountable governmental authority").

[60] *See, e.g.,* British Columbia Ministry of Labour and Citizens' Services, Privacy Guidelines for Use of Video Surveillance Technology by Public Bodies, http://www.mser.gov.bc.ca/privacyaccess/main/video_security.htm.

[61] Alberta Freedom of Information and Protection of Privacy Office, *Guide to Using Surveillance Cameras in Public Areas* (June 2004), http://www3.gov.ab.ca/foip/other_resources/publications_videos/surveillance_guide.cfm.

[62] *See, e.g.,* New South Wales Government Policy Statement and Guidelines for the Establishment and Implementation of Closed Circuit Television (CCTV) in Public Places, NSW Attorney General's Department (2000), *available at* http://www.lawlink.nsw.gov.au/lawlink/cpd/ll_cpd.nsf/vwFiles/cctv.pdf/$file/cctv.pdf.

[63] Council of the Dist. of Columbia, Draft Report, *Investigation of the Metropolitan Police Department's Policy and Practice in Handling Demonstrations in the District of Columbia* (Mar. 11, 2004), *available at* http://www.dccouncil.washington.dc.us/patterson/pages/prinfo/MPDreport31104.doc.

[64] ABA Standards, *supra* note 55, Standard 2-9(1)(d)(iv).

[65] *See* notes 37–39, *supra*.

[66] This process has its roots in the environmental impact reports required of federal agencies when recommending or planning any proposal that will have a significant effect on the quality of the human environment. *See* 42 U.S.C. § 4332(c). Similarly, the E-Government Act of 2002 requires that federal agencies produce a Privacy Impact Assessment (PIA) before they develop or use information technology that collects, maintains, or disseminates personally identifiable information. Pub. L. No. 107-347, § 208, 116 Stat. 2899, 2921–2922. The PIA must address what information is to be collected and why, the intended use of the information, with whom the information will be shared, what notice or opportunities for consent will be provided to individuals regarding their information, how the information will be secured, and whether a system of records is being created under the Privacy Act. § 208(b)(2)(B)(ii).

This process also has similarities to the PIA required by many Canadian provincial governments for public use of video surveillance. Under those guidelines, the authority seeking to implement the system will create a report outlining the expected impact of the system on privacy and other rights and liberties (as per Canadian law). The report and any arguments in favor of the system are sent to the provincial Privacy Commissioner for review and approval. *See, e.g.,* Alberta Freedom of Information and Protection of Privacy Office, *Guide to Using Surveillance Cameras in Public Areas* (June 2004), http://www3.gov.ab.ca/foip/other_resources/publications_videos/surveillance_guide.cfm.

[67] The following requirements are in part an elaboration on the standard developing in the federal courts in an attempt to apply ECPA to video surveillance. This standard has been adopted by a number of federal courts of appeal. *See, e.g., United States v. Williams,* 124 F.3d 411 (3d Cir. 1997); *United States v. Falls,* 34 F.3d 674 (8th Cir. 1994); *United States v. Koyomejian,* 970 F.2d 536 (9th Cir. 1992); *United States v. Torres,* 751 F.2d 875 (7th Cir. 1984).

[68] A surveillance database with identified individuals could be considered a "system of records," which, when undertaken by a federal agency, falls under the Privacy Act of 1974. The Privacy Act imposes rules and restrictions for such records, including rules related to disclosure to third parties, subject rights of access, and criminal and civil remedies. *See* Privacy Act of 1974, 5 U.S.C § 552a. *See also* Section III.C.7., *infra*.

[69] *See generally* 2 Wayne R. LaFave, Search and Seizure: A Treatise on the Fourth Amendment (4th ed. West 2004) (covering the probable cause standard and search warrants).

[70] *See* 3 LaFave, *supra* note 69, at 671–74.

[71] Exclusion of improperly obtained evidence is mandatory where the evidence was gathered in violation of the Fourth Amendment. *See* 1 LaFave, *supra* note 69, at 3–5. Exclusion is also required in certain situations imposed by statute, such as in the Wiretap Act and ECPA. *See* 18 U.S.C. § 2515.

[72] Because of the difficulty of proving actual damages in privacy cases, many privacy statutes impose statutorily defined "liquidated" damages. *See, e.g.,* Video Privacy Protection Act, 18 U.S.C. § 2710; Drivers Privacy Protection Act, 18 U.S.C. § 2721.

[73] ECPA provides this type of damages for violations of its terms. *See* 18 U.S.C. § 2510. It should be noted that a recent Supreme Court case, *Doe v. Chao,* calls into question the ability of plaintiffs to receive statutory damages without also proving actual harm. 540 U.S. 614 (2004).

MODEL LEGISLATION FOR ESTABLISHING PUBLIC VIDEO SURVEILLANCE SYSTEMS

The Constitution Project offers this model legislation to codify the recommendations in the *Guidelines for Public Video Surveillance*. This model code provides legislative language to enable state and local government officials to adopt these recommendations with ease. We are grateful to the Samuelson Law, Technology & Public Policy Clinic at U.C. Berkeley's Boalt Hall School of Law, for their extensive work in drafting this model legislation.

We hope that communities considering implementation of Public Video Surveillance Systems will use this model legislation in establishing such systems in their own jurisdictions.

PUBLIC VIDEO SURVEILLANCE SYSTEMS

Article 1: General Provisions

Section 101. Findings.

The [legislature/governing body] finds and declares as follows:

a. Public video surveillance technology may offer communities potentially useful tools for preventing, deterring, and investigating terrorism and crimes.

b. These systems and new technologies also create the possibility of more intrusive forms of surveillance, with the potential to upset the existing balance between law enforcement needs and constitutional rights and values.

c. Modern video surveillance must be balanced with the need to protect our core constitutional rights and values, including among others privacy and anonymity, free speech and association, government accountability, and equal protection.

d. Lawmakers should ensure that new surveillance capabilities conform to constitutional rights and values.

Section 102. Purpose.

a. The purpose of this [act] is to ensure that all public video surveillance systems:

   1. further a legitimate, clearly articulated law enforcement purpose;
   2. can effectively achieve their articulated purpose;
   3. can achieve their articulated purpose more efficiently than could alternative means;
   4. minimally impact constitutional rights and values;
   5. employ an open and publicly accountable review, approval, and implementation process; and
   6. employ technological and administrative safeguards to reduce the potential for Misuse and abuse of the System.

b. Systems that do not meet the above qualifications should not be approved.

Section 103. Definitions.

"Appending Data" means using technology to attach personally identifiable information, such as name, address, or criminal history, to Footage or other records of the Public Video Surveillance System such that those subsequently accessing the Footage or records can also access attached personal information.

"Automatic Identification" means use of a Public Video Surveillance System in conjunction with biometric or other digital technologies to ascertain or confirm the identity of an individual whose image is captured on Video Surveillance Footage, whether in real time, as applied to Recorded Footage, or prospectively.

"Automatic Tracking" means the use of a Public Video Surveillance System to follow a specific individual or his or her vehicle with technology operating independently of immediate or direct human control, regardless of whether his or her identity is known, so as to create a seamless record of his or her activity during a specific period.

"Community Group" means a locally-based organization representing residential, recreational, economic, or other interests of those individuals living and working in the area to be surveilled and its adjacent neighborhoods.

"Governing Body" means the local elected officials accountable to the jurisdiction for which a Public Video Surveillance System is being considered. This may include, but is not limited to, such bodies as the City Council, Board of Supervisors, State Legislature, Office of the Mayor, or other Executive office.

"Harm" means physical, financial or emotional injury and is not limited to legal wrongs or violations of legal duties.

"Initial Review" means any review of Footage occurring at the same time, or within [one hour], of the occurrence of the actual events in the Video Surveillance Footage.

"Installation" means an arrangement of cameras allowing them to operate without direct manual control.

"Interest Group" means an organization advancing issue-based concerns, including but not limited to civil liberties, community safety, privacy, racial justice, economic justice, needs of the homeless and seniors. Interest Groups need not be locally based.

"Misuse" means use, operation of or interaction with a PVS System in a manner inconsistent with the use restrictions described in Article III of this statute or otherwise not conforming to the approved purposes of the PVS System.

"Observation" means real-time viewing of live camera images.

"Operating Agency" means the governmental agency or other entity responsible for using and/or maintaining the Video Surveillance System. In most cases this will be the local law enforcement agency.

"Operator" means a person authorized to use the System, working for or under the supervision or control of the Operating Agency.

"Pan, Tilt, and Zoom" means manipulating a camera to view areas outside the original image frame or measurably increase the resolution of the images rendered.

"Permanent Public Video Surveillance System" or "PPVS System" means an Installation of one or more government owned and operated video cameras focused on a public place, not handheld by System Operators, implemented for an indefinite period of time or for longer than [240 days—the maximum time permitted for a Temporary Public Video Surveillance System pursuant to Section 210 of this model legislation], and the primary purpose of which extends beyond a single, specific law enforcement investigation.

"Public Video Surveillance System" or "PVS System" or "System" means one or more government owned and operated cameras focused on a public place and remotely operated.

"Recorded" refers to images that are preserved and stored by a Public Video Surveillance System for later review. This includes preservation for any length of time beyond a short window necessary to perform an "Initial Review" of the Footage.

> ***Legislative Note:*** *This definition is intended to permit camera monitors to quickly re-wind and re-play Footage, or to quickly review Footage that is temporarily Recorded during a one-hour lunch break (see one hour period in definition of "Initial Review"), without considering that Footage Recorded, provided that the images are not preserved beyond that one-hour time period.*

"Reviewer" means the "Governing Body" or a commissioner or commission appointed by the Governing Body that reviews proposals and executes the "Impact Assessment" pursuant to Sections 202–209.

"Secondary Purpose" means an intentional, planned use of a System, a component of it, or the collected data, for a purpose other than an original approved purpose for the System.

"Targeted Public Consultation" means the process of meeting and conferring with a cross section of "Community Groups" and "Interest Groups" for the purpose of seeking guidance on the design of a Public Video Surveillance System, Section 206.

"Temporary Public Video Surveillance System" or "TPVS System" means a Public Video Surveillance System not considered a Permanent Public Video Surveillance System.

"Third Parties" means individuals or entities (other than the individual requesting access to records relating to his or her self) that are not under the supervision or control of the Operating Agency.

"Video Surveillance Footage" or "Surveillance Footage" or "Footage" means any images Recorded by a Public Video Surveillance System including time and location data and any additional metadata or information appended to the images on the Footage.

Article 2: Procedures for Review, Approval, and Implementation of Public Video Surveillance Systems

Part 1. Public Video Surveillance Systems— Authority to Review, Approve and Implement.

Section 201. Authority to Review, Approve and Implement PVS Systems.

a. The Governing Body shall retain non-delegable authority to approve implementation of Permanent Public Video Surveillance Systems. Law enforcement, a member of the public, or the Governing Body itself may initially suggest implementation of a Permanent Public Video Surveillance System. To draft the formal proposal to implement such a System, the Governing Body may, at its option:

   1. appoint an independent commissioner or commission to draft proposals for Public Video Surveillance Systems and execute Impact Assessments; or

   2. retain authority to draft proposals and execute Impact Assessments.

b. Operators of prospective Temporary Public Video Surveillance (TPVS) Systems may seek approval of the Governing Body through the Impact Assessment, Sections 203–209, or pursuant to an order from a court of competent jurisdiction in accordance with the provisions of Section 210 (Approval of Temporary Public Video Surveillance Systems).

Part 2. Permanent Public Video Surveillance Systems—Impact Assessment Required.

Section 202. Impact Assessment Required for Permanent Public Video Surveillance Systems.

a. Except as provided in Section 212 (Systems with Limited Technological Capabilities), no Permanent Public Video Surveillance (PPVS) System shall be approved or installed unless a completed Impact Assessment, Sections 203–209 (PVS Impact Assessment), is on file with the Governing Body.

b. The Impact Assessment shall serve as the evaluative basis for all decisions to approve and implement Permanent Public Video Surveillance Systems.

Part 3. Public Video Surveillance Impact Assessment.

Section 203. Public Video Surveillance Impact Assessment.

a. The PVS Impact Assessment shall consist of five steps:

   1. PVS Proposal, Section 204.
   2. Public input on PVS Proposal, Section 205.
   3. Draft PVS Impact Report, Section 208.
   4. Period of Public Comment on Draft PVS Impact Report, Section 207.
   5. Final PVS Impact Report, Section 209.

b. Impact Assessment proceedings shall be subject to the [state public records act, open meetings laws, sunshine acts in jurisdiction]. Meetings held pursuant to Targeted Public Consultation, Section 206, need not be open to the public, but still must meet the public disclosure requirements specified in Section 206(b) (Targeted Public Consultation).

Section 204. PVS Proposal.

a. Initial Proposal Required. The Impact Assessment of a PVS System begins with an initial proposal outlining the intended purpose and scope of the System, prepared by the Reviewer.

b. The proposal shall include:

   1. articulation of the legitimate law enforcement purposes that justify the System; and

   2. details of the technological design and geographical scope of the System, including locations on which cameras are to be focused, the visual coverage of the System, and the proposed technical specifications of the entire System.

   3. Proposals detailing Systems that exhibit limited technological capabilities as described in Section 212 shall be subject to the review processes described therein, and need only comply with the remainder of the PVS Impact Assessment, Sections 205–209, to the extent noted in Section 212.

   Legislative Note: *This model statute does not specify standards for whom or what agencies can suggest a PVS System. Rather, provision (a) provides that whether law enforcement, another government agency or a citizens' group initially suggests a PVS System, the Reviewer shall be responsible for drawing up a proposal that details its intended purpose and scope. This insures that descriptions of planned Systems will be sufficiently detailed that they can be effectively evaluated by members of the public.*

Section 205. Public Input Required.

a. Public input is required on the PVS Proposal and will inform the Draft PVS Impact Report. The Reviewer shall solicit public input on the PVS Proposal through either Targeted Public Consultation, Section 206, or a period of Public Comment, Section 207.

b. A period of Public Comment on the Draft PVS Impact Report is required and will inform the Final PVS Impact Report.

Section 206. Targeted Public Consultation.

a. Targeted Public Consultation shall consist of meetings or other communication offering a broad cross-section of Community and Interest Groups the opportunity to review and comment on the PVS Proposal.

b. The Reviewer shall make public:

1. a list of entities and individuals participating in targeted consultations;
2. all documents passed between Community and Interest Groups and the Reviewer during the targeted consultation process; and
3. summary notes of meetings taken as a part of the Targeted Public Consultation process.

Section 207. Public Comment.

a. The Reviewer shall facilitate public comment.

b. The report or proposal on which comment is sought shall be made available to the public via local government print and electronic publications. Local press outlets shall be notified and local regulations with respect to public hearings and soliciting public comments shall apply.

c. The Reviewer shall provide a reasonable period of time for meaningful public comment. This time period shall be at least [60] days.

d. Public comment shall include opportunity for members of the public to submit written comments and at least one public hearing held in accordance with relevant local regulations for public hearings.

e. The Reviewer will compile a complete written record of public comment.

f. Following the period of public comment:

   1. If comments applied to the PVS Proposal, the Reviewer will prepare the Draft PVS Impact Report, Section 208.
   2. If comments applied to the Draft PVS Impact Report, the Reviewer will revise the report in light of public comments, including altering recommendations if appropriate. The Reviewer will then submit the revised report and indexed public comments to the Governing Body to facilitate decision-making.

   Legislative Note: *Public Comment on the PVS Proposal is optional, and may be substituted for by Targeted Public Consultation, see Section 205(a) and 206, supra. Public Comment on the Draft PVS Impact Report is mandatory, see Section 205(b), supra, and 208, infra.*

Section 208. Draft PVS Impact Report.

a. Following the Targeted Public Consultation or public comment required under Section 205 (Public Input Required), the Reviewer shall prepare and make available to the public a comprehensive report to be known as the Draft PVS Impact Report.

b. The Draft PVS Impact Report shall address specific issues raised by the public during consultation or comment and shall include:

   1. Articulation and evaluation of the legitimate law enforcement purposes that justify the System.

   2. Details of the technological design and geographical scope of the System, including locations to be surveilled, the visual coverage of the System, and the proposed technical specifications of the System.

   3. Analysis of whether and how the proposed System will effectively address its purposes.

   4. Assessment of the proposal's cost, including initial outlay, projected maintenance expenses and personnel costs.

   5. Comparison of the cost and utility of the System to alternative means of attaining the same purpose.

   6. Analysis of the impact of the System on constitutional rights and values, including:

      i. privacy and anonymity;

      ii. freedom of speech and association;

      iii. government accountability;

      iv. due process;

      v. equal protection.

   7. Assessment of potential incidental costs or benefits of the System and their likelihood.

   8. Analysis of possible "spillover effects," or consequences of the System for areas not surveilled, including the possibilities of crime increases in adjacent neighborhoods.

   9. With the foregoing factors in mind, an overall cost-benefit analysis of the proposed System. This may include, where appropriate, an analysis of the PVS experiences of similar cities or cities with similar Systems, including relevant similarities or differences of those cities and their Systems.

   10. A recommendation to guide the decision of the Governing Body.

c. All communications material to the Reviewer's recommendation, including all communications with outside individuals and groups, shall be introduced on the record in the Draft PVS Impact Report.

Section 209. Final PVS Impact Report.

a. Based on the Draft PVS Impact Report, the Targeted Consultation and the public comment period(s), the Governing Body will determine whether to approve, modify or reject the proposed PVS System within a reasonable span of time. In order to facilitate its decision, the Governing Body may request from the Reviewer, Community and Interest Groups or government agencies additional information about potential costs, benefits or effects of the System, or may choose to hold a public hearing.

b. The Governing Body will modify the revised Draft PVS Impact Report as appropriate and issue it publicly as a Final PVS Impact Report. This report will include a section stating the Governing Body's final decision and the basis for that decision. All communications material to the Governing Body's final decision, including all communications with outside individuals and groups, shall be introduced on the record in the Final PVS Impact Report.

Part 4. Temporary Public Video Surveillance Systems—Approval by Impact Assessment or Court Order.

Section 210. Approval of Temporary Public Video Surveillance Systems.

a. Approval for a Temporary Public Video Surveillance (TPVS) System may be sought through the Impact Assessment, Sections 203-209, or pursuant to an order from a court of competent jurisdiction. Each application for a court order authorizing Temporary Public Video Surveillance shall be made in writing upon oath or affirmation of the [Attorney General, Chief Deputy Attorney General, a district attorney, or an individual within the Operating Agency authorized by any of the above persons].

b. Applications for a court order shall state or describe each of the following:

   1. the identity of the individual making the application, and of the [Operating Agency] that is to execute the order;

   2. the law enforcement purposes of the proposed System, and how the Surveillance System is likely to produce evidence useful in serving these purposes;

3. other means attempted or considered to investigate or combat the crimes at issue, and explanations of why they have been or are likely to be unsuccessful or impractical;
4. reasons the purpose of the System would be frustrated by the Impact Assessment process;
5. the time period for which the System is to be deployed, which shall not exceed [120 days];
6. the places and activities to be surveilled, and a description of why surveillance of those locations is expected to further law enforcement objectives; and
7. any protections or safeguards incorporated into the System design to minimize the intrusion into the constitutional rights and values of individuals whose images will be captured by the surveillance.

c. The court shall grant a "Temporary Video Surveillance Order" if it is persuaded that:

1. the articulated law enforcement purposes of the System are legitimate;
2. the Surveillance System is likely to produce evidence useful in serving these purposes;
3. the planned surveillance could reasonably be considered likely to be more effective or less dangerous than other available means of investigating or combating the crimes at issue;
4. there is a public interest in rapid deployment or secrecy of the TPVS System that would be compromised by the public comment process;
5. the proposed System will be deployed for a limited time no longer than reasonably necessary to achieve the stated objectives, and not exceeding [120 days];
6. the System will feature no greater scope or capabilities than reasonably necessary to achieve a legitimate law enforcement purpose;
7. surveillance of the stated locations is reasonably necessary to further the System's legitimate law enforcement objectives; and
8. reasonable protections and safeguards will be taken to minimize intrusion into the constitutional rights and values of individuals whose images will be captured by the surveillance, but who are not suspected of criminal activity.

d. When amendments to System design could allow a proposed System to meet the above requirements and still fulfill the purpose of the System, courts may require such amendments rather than reject applications for TPVS outright.

e. A court approving a TPVS System will issue a "Temporary Video Surveillance Order," specifying the time period and locations to be surveilled.

f. The Operator may file a time period extension request with a court of competent jurisdiction, which may at its discretion require evidence demonstrating need or issue a written judgment on the basis of the written request.

   1. The time period covered by the extension shall not exceed [the maximum number of days specified in Subsection (c)(5) above. 120 in this model statute].

   2. No requests for extensions shall be granted that will result in a TPVS System operating for more than [the maximum number of days specified in Subsection (c)(5) above, plus the maximum extension period. This shall be the maximum number of days allowed for operation before a temporary System will be considered a permanent System for purposes of this statute. 240 days in this model statute.] total days.

      i. A System shall be considered in operation from the day it is first turned on for use until the day it is permanently turned off to be dismantled. Interim periods during which the System may be temporarily turned off count as time in which the System is in operation, and count against the maximum number of days available for a System to be considered temporary.

      ii. Systems operated longer than [the maximum TPVS period—240 days in this model statute] shall be considered permanent Systems for the purposes of this statute, and shall be subject to the requirements of Subsection (f)(3) of this Section.

   3. Operators seeking to extend the operation of a TPVS System beyond the maximum period of days must:

      i. prior to the expiration of the maximum period set forth in Subsection (f)(2), apply to the court for a second extension to cover the time period necessary for completing the Impact Assessment process under Sections 203–209.

      ii. seek approval of the System through the Impact Assessment process set forth in Sections 203–209.

   4. Temporary Systems initially approved under the Impact Assessment (rather than by court order), and now seeking approval as permanent Systems, shall be considered to have changed their purpose, and shall be reviewed in accordance with the provisions of Section 215, Change in Purpose of Public Video Surveillance System.

Legislative Note: *As above with respect to Automatic Identification, localities should feel free to adapt this Section to conform to state or local rules or practices regarding obtaining warrants or other court orders.*

Section 211. Approval of Temporary Public Video Surveillance Systems Under Exigent Circumstances.

a. Upon informal application by the [Attorney General, Chief Deputy Attorney General, a district attorney, or an individual within the Operating Agency authorized by any of the above persons], a [judge of competent jurisdiction] may grant oral approval for a Temporary Public Video Surveillance System, without an order, if he or she determines all of the following:

   1. There are grounds upon which an order could be issued under this chapter.
   2. There is probable cause to believe that an emergency situation exists.
   3. There is probable cause to believe that a substantial danger to life or limb exists justifying the authorization for immediate public video surveillance before an application for an order could with due diligence be submitted and acted upon.

b. If the person seeking oral approval for public video surveillance under this Section is unable, after a good faith effort, to contact a [judge of competent jurisdiction], such person may authorize and proceed with the emergency employment of a Temporary Public Video Surveillance System without an order, if he or she determines all of the following:

   1. There are grounds upon which an order could be issued under this chapter.
   2. There is probable cause to believe that an emergency situation exists.
   3. There is probable cause to believe that a substantial danger to life or limb exists justifying the authorization for immediate public video surveillance before an application for an order could with due diligence be submitted and acted upon.

c. Approval for a Temporary Public Video Surveillance System under this Section shall be conditioned upon filing with the judge, within 72 hours of the oral approval under Subsection (a) of this Section or a determination under Subsection (b) of this Section, a written application for an order which, if granted consistent with this chapter, shall also recite the oral approval under Subsection (a) or determination under Subsection (b) and be retroactive to the time of such oral approval or determination.

Part 5. Systems With Limited Technological Capabilities—Alternative Impact Assessment Available.

Section 212. Alternative Impact Assessment for PVS Systems With Limited Technological Capabilities.

a. The Governing Body may elect to perform an Alternative Impact Assessment in place of the PVS Impact Assessment if and only if the Reviewer concludes in the PVS Proposal that the System incorporates the following safeguards:

   1. Data gathered by the Video Surveillance System is automatically deleted after [96 hours] (or earlier), unless specific data is requested by law enforcement pursuant to Section 314.

   2. The Video Surveillance System does not have Automatic Tracking or Identification capabilities.

   3. Data gathered by the Video Surveillance System is protected by adequate data security measures for the duration of its retention, pursuant to Section 325.

   4. The video surveillance data is unavailable to Third Parties except as provided in Sections 315, 320–324.

b. The Alternative Impact Assessment shall include:

   1. A combined PVS Proposal and Draft PVS Impact Report, Sections 204 and 208. The Draft Report may *exclude* the assessment of "potential incidental costs or benefits of the System and their likelihood" otherwise required pursuant to Section 208(b)(7).

   2. A period of Public Comment, Section 207.

   3. A Final PVS Impact Report, Section 209.

c. The Alternative Impact Assessment need not include Targeted Public Consultation.

Legislative Note: *The Alternative Impact Assessment thus consolidates the PVS Proposal and the Draft PVS Impact Report. The Reviewer may simultaneously author both the Proposal and Draft Report, forego Targeted Public Consultation, and advance immediately to Public Comment. This should save significant time and resources, and provides an incentive for jurisdictions to consider limiting their Systems' technological capacity. This in turn helps safeguard the constitutional interests of citizens. Note also that one example of data security measures would be encryption at the moment of recording.*

Part 6. Existing Systems—Periodic Audits Required, Review in Case of Misuse or Harm, Alterations or Change in Purpose.

Section 213. Periodic Audits Required.

a. The Reviewer will conduct a periodic review of implemented PVS Systems to assess each System's effectiveness, impact on the community, and adherence to the System's stated primary purpose.

   1. The Reviewer will publicly announce its intention to conduct an audit and provide instructions as to how individuals and organizations can submit comments or seek meetings.

   2. The Reviewer is not obligated to hold public hearings or to solicit meetings with Community and Interest Groups.

   3. The Reviewer will accept written comments submitted by members of the public and will grant meetings to Community and Interest Groups upon request as appropriate.

   4. The Reviewer will consult the Operating Agency, System records, complaints, disciplinary records, and other records to determine the extent to which the System has:

      i. assisted law enforcement in advancing the purposes for which the PVS was established;

      ii. been Misused; or

      iii. been used for Secondary Purposes.

   5. In light of the Reviewer's findings and comments submitted, the Reviewer (if separate from the Governing Body) will recommend to the Governing Body whether to renew, cancel, or alter the System.

   6. The Governing Body will issue a public report stating its decision to renew, cancel, or alter the System in order to resolve or ameliorate problems identified by the audit. The report will detail the reasons for its decision, with specific references to the Reviewer's findings and conclusions and comments submitted. Decisions to significantly alter the System by removing key limitations on its technological capacity or otherwise significantly increasing its potential for invasive use are subject to immediate review under the Alternative Impact Assessment.

b. The reviewing period will be established by the Governing Body and will not exceed [a reasonable time period to be established by the jurisdiction, but no longer than two years] between reviews.

Section 214. Systems Already in Existence at Passage of This Act.

Pre-existing PVS Systems shall be reviewed in accordance with procedures for periodic audits, Section 213, and must undergo such a review within one year of adoption of this Act.

Section 215. Change in Purpose of Public Video Surveillance System.

a. If the primary law enforcement purpose of a PVS System changes, it shall be immediately reviewed under the Alternative Impact Assessment under Section 212.

b. A change in purpose may be found either:

   1. explicitly, where a new purpose for the Public Video Surveillance System is announced by the Operator; or

   2. implicitly, where during review under Section 213, 214, 216 or 217, it comes to the Reviewer's attention that requests for access to or retention of Footage for legitimate law enforcement Secondary Purposes occur with approximately equal or greater frequency than requests serving the System's primary purpose.

Section 216. Review Required in Cases of Misuse and Harm.

a. A PVS System shall be subject to an immediate audit when credible evidence is brought to the attention of the Governing Body or Reviewer demonstrating:

   1. use or Misuse of a PVS System by any individual(s) resulting in grave Harm to a person when such Harm is not the necessary and legitimate outcome of a legitimate law enforcement investigation; or

   2. repeated and similar instances of use or Misuse of a PVS System by multiple Operators resulting in Harm to others when such Harm is not the necessary and legitimate outcome of a legitimate law enforcement investigation.

b. Pending results of the audit, the Governing Body shall have the discretion to suspend the System.

c. The Reviewer will examine features of the System contributing to Misuse and consult with legal and technical experts, Community and Interest Groups, or others as appropriate.

d. The Reviewer shall issue a public report of findings and recommendations, except that certain findings may remain confidential to the extent necessary to protect ongoing investigations.

e. The Governing Body will consider the recommendations in determining whether to alter or cancel the System, and whether to refer the matter for disciplinary action.

> ***Legislative Note:*** *The criteria above are intended primarily to encapsulate two scenarios. The first is action by a single individual resulting in serious Harm to others. This would indicate that the System has the capacity to do serious Harm when Misused, and thus should be reviewed for means to reduce this Harm. The second scenario envisions multiple occurrences of similar types of abuse or Misuse. Even if the individual incidents do not result in especially serious Harm to individuals, the repetitive nature of the Misuse may indicate a flaw in the System that ought to be remedied.*
>
> *Relevant factors in determining whether to suspend, alter or cancel the System may include whether the alleged abuse is likely to continue and to be sufficiently pervasive or serious to outweigh the benefits of maintaining operation.*

Section 217. Review Required After Alterations to Existing Systems.

When alterations are made to a technologically limited PVS System approved under the Alternative Impact Assessment, Section 212, and the alterations remove technological limitations permitting the System to qualify for the Alternative Impact Assessment, the altered System shall be immediately subject to a PVS Impact Assessment, Sections 203–209.

Part 7. Sanctions—Compliance With Review Process.

Section 218. Enforcement by State Attorney General.

a. The state Attorney General or equivalent state review panel shall be empowered to investigate and review failures to comply with the provisions of this article, and to issue orders for compliance.

b. Upon a finding of failure to comply, the state may withhold funds from the Operating Agency until compliance is attained.

Section 219. Private Right of Action.

a. Any resident of the jurisdiction subject to the authority of the Governing Body may commence a civil action on his or her own behalf against the Governing Body for failure to comply with the provisions of this article.

b. Remedies available to such a plaintiff shall include:

1. Issuance of an injunction limiting or barring further use of the Surveillance System until compliance is achieved.
2. Provision of reasonable attorney's fees.

Legislative Note: *Nothing in this legislation prohibits plaintiffs claiming injuries caused by use or Misuse of a PVS System from introducing failure to comply with the provisions of this article as evidence.*

Article 3: Use Restrictions

Part 1. Restricted Use of Recording, Automatic Identification, Automatic Tracking, and Pan, Tilt, and Zoom.

Section 301. Specifications of System.

Public Video Surveillance Systems shall conform to the specifications outlined in a Final PVS Impact Report under Section 209 or court order under Section 210.

Legislative Note: *Although careful planning and analysis of a Public Video Surveillance System's technical specifications is important, it is also essential that the System as built conforms to those specifications.*

Section 302. Automatic Identification Prohibited Absent Authorization.

Except as provided in Sections 303, 309, and 310, using a Public Video Surveillance System for purposes of Automatic Identification is prohibited.

> ***Legislative Note:*** *The use of Automatic Identification technology raises specialized concerns regarding constitutional rights and values. Even in public, most people expect to remain anonymous unless they are seen, recognized, and remembered by another individual present in that location. Pervasive use of automated identification undermines this expectation—implicating privacy, anonymity, and First Amendment freedoms. Thus, use of Automatic Identification should be permissible only after obtaining a court order in accordance with the rules and procedures set forth in Section 303 or pursuant to the exigency and federal counterterrorism exceptions in Section 309 and 310.*

Section 303. Order Authorizing Automatic Identification.

a. Each application for an order authorizing Automatic Identification using a Public Video Surveillance System shall be made in writing upon oath or affirmation of the [Attorney General, Chief Deputy Attorney General, a district attorney, or an individual within the Operating Agency authorized by any of the above persons] to [a judge of competent jurisdiction]. Each application shall include all of the following information:

    1. the identity of the individual making the application, and of the [Operating Agency] that is to execute the order;

    2. a full and complete statement of the facts and circumstances relied on by the applicant to justify his or her belief that such an order should be issued, including:

        i. details regarding the particular offense that has been, is being, or is about to be committed;

        ii. a particular description of the location or locations of such offense; and

        iii. the identity, if known, or a description of the person(s) believed to be involved in the commission of the offense and who is (are) to be identified;

    3. a statement of the period of time over which the Automatic Identification is to be performed, including whether the identification is to be performed retroactively on existing Footage, is to be applied on a continuing basis, or both;

    4. a full and complete statement of the facts concerning all previous applications for Automatic Identification known to the individual authorizing and making the

application involving any of the same persons or particular offenses specified in the application, and the action taken by the judges on these applications; and

5. if the application is for the extension of an order authorizing Automatic Identification, a statement setting forth the results of the Automatic Identification under the original order, or a reasonable explanation of the failure to obtain results.

b. The judge may require the applicant to furnish additional testimony or documentary evidence in support of an application for an order under this Section.

c. Upon application made under this Section, the judge may enter an *ex parte* order, as requested or modified, authorizing Automatic Identification within the territorial jurisdiction of the court in which the judge is sitting, if the judge determines, on the basis of the facts submitted by the applicant, all of the following:

1. There is probable cause to believe that an individual is committing, has committed, or is about to commit an offense, the investigation and/or prevention of which is consistent with the purpose of the System as articulated in the Final PVS Impact Report, or use for an approved Secondary Purpose, if the required showing under Section 317 has also been made.

2. There is probable cause to believe that evidence of or information about that crime or the individual who is suspected of committing or planning that crime will be obtained through the use of Automatic Identification as described in the application.

3. Other investigative techniques have been tried and were unsuccessful, or such techniques reasonably appear to be unlikely to succeed or to be impractical.

d. *Time Period Authorized:* For requests for Automatic Identification covering already existing Footage, the application must justify the time period contained within the request to demonstrate that it serves the purposes outlined under Subsection (c) of this Section. For requests for Automatic Identification on Footage that has not yet been Recorded, the maximum authorized time period for Automatic Identification shall be 30 days (measured either in real time or in duration of Recorded Footage). Extensions of an order may be granted, but only upon application for an extension made in accordance with Subsection (a) of this Section, and upon the court making findings required by Subsection (c) of this Section. The period of extension shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event any longer than 30 days.

e. Each order authorizing Automatic Identification shall specify all of the following:

1. a particular description of the person(s) to be automatically identified;

2. a description of the location(s) of the camera(s) or of the location(s) depicted in the Footage on which the Automatic Identification is to be performed;
3. the identity of the [Operating Agency] authorized to perform the Automatic Identification; and
4. the period of time during which such Automatic Identification is authorized, including whether the identification is to be performed retroactively on existing Footage, is to be applied on a continuing basis, or both, and if the order is for extension of a previous order, the period of time during which Automatic Identification has already been performed.

Legislative Note: *Localities should adapt this Section as appropriate to conform to state or local rules or practices regarding obtaining warrants or other court orders.*

Section 304. Appending Data to Public Video Surveillance Footage Prohibited.

Except as provided in Section 305, Appending Data to Public Video Surveillance Footage is prohibited.

Section 305. Operator Guidelines for Appending Data.

a. The Operating Agency shall promulgate clear and specific guidelines detailing the situations in which it is appropriate to append data to Public Video Surveillance Footage, provided that no Automatic Identification may be performed except pursuant to the terms of Section 303. The Operating Agency may provide for less stringent standards for appending identification data obtained through personal Observation or other non-automated methods.

b. Any Operator who violates the Operator's guidelines for Appending Data to Public Video Surveillance Footage shall be subject to administrative discipline under Section 328.

Section 306. Notification of Individuals Subject to Identification on Surveillance Footage.

a. Within a reasonable time, but no later than 90 days, after the termination of the period of an order authorizing Automatic Identification or extensions thereof, or after personally identifiable information about an individual has been appended to Video Surveillance Footage, the Operating Agency shall serve upon persons who have been identified in Surveillance Footage an inventory which shall include notice of all of the following:

1. The fact of entry of the order or appending of identifying information.
2. The date of the entry of the order or appending of information, and the period of time covered by the order or Footage.

b. The judge, upon the filing of a motion, may, in his or her discretion, make available to the person identified or his or her counsel for inspection the portions of Footage on which Automatic Identification techniques have been performed, and any information resulting from the Automatic Identification, which the judge determines to be in the interest of justice.

c. On an *ex parte* showing of a legitimate law enforcement purpose to a judge, the serving of the report required by this Section may be postponed. The period of postponement shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted.

d. A criminal defendant shall be notified that he or she was identified as a result of Automatic Identification that was performed pursuant to this chapter. The notice shall be provided prior to the entry of a plea of guilty or nolo contendere, or at least 20 days prior to any trial, hearing, or proceeding in the case other than an arraignment or grand jury hearing; provided that if the defendant would otherwise be entitled to receive such information earlier under state rules of criminal procedure, the earlier disclosure requirements shall apply.

Legislative Note: *Reports of instances of Automatic Tracking are not subject to this notice requirement, to the extent that Automatic Tracking occurs without Automatic Identification. If Automatic Identification occurs in conjunction with Automatic Tracking, the notice obligation would apply.*

Section 307. Automatic Tracking.

Except as provided in Sections 308, 309, and 310, using a Public Video Surveillance System for purposes of Automatic Tracking or Appending Data to Public Video Surveillance Footage is prohibited.

Section 308. Order Authorizing Automatic Tracking.

a. Each application for an order authorizing Automatic Tracking using a Public Video Surveillance System shall be made in writing upon oath or affirmation of the [Attorney General, Chief Deputy Attorney General, a district attorney, or an individual within

the Operating Agency authorized by any of the above persons] to [a judge of competent jurisdiction]. Each application shall include all of the following information:

1. The identity of the individual making the application, and of the [Operating Agency] that is to execute the order;
2. A full and complete statement of the facts and circumstances relied on by the applicant to justify his or her belief that such an order should be issued, including:
   i. details regarding the particular offense that has been, is being, or is about to be committed;
   ii. a particular description of the location or locations of such offense; and
   iii. the identity, if known, or a description of the person(s) believed to be involved in the commission of the offense and who is (are) to be tracked;
3. A statement of the period of time over which the Automatic Tracking is to be performed, whether the Automatic Tracking is to be performed retroactively on existing Footage, is to be applied on a continuing basis, or both;
4. A full and complete statement of the facts concerning all previous applications for Automatic Tracking known to the individual authorizing and making the application involving any of the same persons or particular offenses specified in the application, and the action taken by the judges on these applications; and
5. If the application is for the extension of an order authorizing Automatic Tracking, a statement setting forth the results of the Automatic Tracking under the original order, or a reasonable explanation of the failure to obtain results.

b. The judge may require the applicant to furnish additional testimony or documentary evidence in support of an application for an order under this Section.

c. Upon application made under Subsection (a) of this Section, the judge may enter an *ex parte* order, as requested or modified, authorizing Automatic Tracking within the territorial jurisdiction of the court in which the judge is sitting, if the judge determines, on the basis of the facts submitted by the applicant, all of the following:

   1. There is probable cause to believe that an individual is committing, has committed, or is about to commit an offense, the investigation and/or prevention of which is consistent with the purpose of the System as articulated in the Final PVS Impact Report, or use for an approved Secondary Purpose, if the required showing under Section 317 has also been made.

2. There is probable cause to believe that evidence of or information about that crime or the individual who is suspected of committing or planning that crime will be obtained through the use of Automatic Tracking as described in the application.

3. Other investigative techniques have been tried and were unsuccessful, or such techniques reasonably appear to be unlikely to succeed or to be impractical.

d. *Time Period Authorized:* For requests for Automatic Tracking covering already existing Footage, the application must justify the time period contained within the request to demonstrate that it serves the purposes outlined under Subsection (c) of this Section. For requests for Automatic Tracking on Footage that has not yet been Recorded, the maximum authorized time period for Automatic Tracking shall be 30 days (measured either in real time or in duration of Recorded Footage). Extensions of an order may be granted, but only upon application for an extension made in accordance with Subsection (a) of this Section, and upon the court making findings required by Subsection (c) of this Section. The period of extension shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event any longer than 30 days.

e. Each order authorizing Automatic Tracking shall specify all of the following:

1. a particular description of the person(s) to be automatically tracked;

2. a description of the location(s) of the camera(s) or of the location(s) depicted in the Footage on which the Automatic Tracking is to be performed;

3. the identity of the [Operating Agency] authorized to perform the Automatic Tracking; and

4. the period of time during which such Automatic Tracking is authorized, including whether the Automatic Tracking is to be performed retroactively on existing Footage, is to be applied on a continuing basis, or both, and if the order is for extension of a previous order, the period of time during which Automatic Identification has already been performed.

Legislative Note: *As above with respect to Automatic Identification, localities should adapt this Section as appropriate to conform to state or local rules or practices regarding obtaining warrants or other court orders.*

Section 309. Automatic Identification or Automatic Tracking Under Exigent Circumstances.

a. Upon informal application by the [Attorney General, Chief Deputy Attorney General, a district attorney, or an individual within the Operating Agency authorized by any of the

above persons], a [judge of competent jurisdiction] may grant oral approval for Automatic Identification or Automatic Tracking, without an order, if he or she determines all of the following:

1. There are grounds upon which an order could be issued under this chapter.
2. There is probable cause to believe that an emergency situation exists.
3. There is probable cause to believe that a substantial danger to life or limb exists justifying the authorization for immediate Automatic Identification or Automatic Tracking before an application for an order could with due diligence be submitted and acted upon.

b. If the individual seeking oral approval for Automatic Identification or Automatic Tracking under this Section is unable, after a good faith effort, to contact a [judge of competent jurisdiction], such individual may authorize and proceed with the emergency employment of Automatic Identification or Automatic Tracking without an order, if he or she determines all of the following:

1. There are grounds upon which an order could be issued under this chapter.
2. There is probable cause to believe that an emergency situation exists.
3. There is probable cause to believe that a substantial danger to life or limb exists justifying the authorization for immediate Automatic Identification or Automatic Tracking before an application for an order could with due diligence be submitted and acted upon.

c. Approval for Automatic Identification or Automatic Tracking under this Section shall be conditioned upon filing with the judge, within 72 hours of the oral approval under Subsection (a) of this Section or a determination under Subsection (b) of this Section, a written application for an order which, if granted consistent with this chapter, shall also recite the oral approval under Subsection (a) or determination under Subsection (b) and be retroactive to the time of such oral approval or determination.

Section 310. Automatic Identification or Automatic Tracking Pursuant to a Federal Counterterrorism Watchlist.

Notwithstanding Sections 302 and 307, an Operating Agency may engage in Automatic Identification and/or Automatic Tracking pursuant to a federal counterterrorism watch list that is part of the Terrorist Screening Database maintained by the federal Terrorist Screening Center (TSC).

Legislative Note: *We recommend creating this exception to the prohibition on Automatic Identification and Automatic Tracking for the use of terrorist watch lists compiled by the federal government. This recommendation is based upon the national security and secrecy concerns underlying the federal lists as well as the practical concern that local officials likely would not be permitted access to the underlying data they would need to justify judicial approval. This exception does not apply to any other watch lists, regardless of source.*

Section 311. Pan, Tilt, or Zoom Prohibited Absent Reasonable Suspicion of Criminal Activity.

a. The Operator shall not use the Pan, Tilt, or Zoom features of a video surveillance camera or System in a way that targets particular individuals absent a reasonable suspicion of criminal activity.

b. The Operating Agency shall promulgate guidelines for the use of Pan, Tilt, or Zoom features of cameras to prevent use of such features in a way that discriminates against individuals on the basis of race, ethnic origin, religion, age, gender, class, economic status, or sexual orientation.

Section 312. Systems Approved for Live Observation Only.

a. Public Video Surveillance Systems approved, according to Article I of this [act], solely for live Observation shall not retain Footage or other data, except for a short period of time during which an Operator performs an Initial Review of Footage, or as required by Section 327.

b. Where a Public Video Surveillance System is capable of recording upon request or instruction of the Operator, the Operating Agency shall promulgate guidelines which limit the circumstances under which recording is permitted, consistent with the purpose of the System as articulated by the [Governing Body] in its Final PVS Impact Report, Section 209.

Legislative Note: *This Section applies to all Systems that are only approved for live Observation, regardless of the method of review undertaken (Impact Assessment, Alternative Impact Assessment, or court order). Put simply, if a System is not approved for recording, it should not be capable of recording.*

Section 313. Pre-archival and Archival Footage—Retention Period.

a. Operating agencies implementing Public Video Surveillance Systems approved for and capable of recording shall designate an initial period during which retained Recorded Footage is considered pre-archival for purposes of Sections 314 and 316–317. The specification of this period shall be based on the Operating Agency's actual practice for completing routine reviews of Recorded Footage, and shall not exceed 7 days.

b. All Footage retained beyond the pre-archival period as specified under subsection (a) of this Section shall be considered archival for purposes of Sections 314 and 316–317.

c. All Footage and accompanying data must be automatically deleted after expiration of 7 days, unless:

   1. Footage is specifically requested for extended retention under Section 314; or

   2. retention of Footage or information is required in order to comply with Section 327.

d. An Operator or Operating Agency shall not be civilly or criminally liable for the destruction of Footage or accompanying data in accordance with the rules established under this Section.

> ***Legislative Note:*** *This Section establishes two different categories of Recorded Footage, which will require different levels of review and authorization before access is allowed to Operators. As a general matter, Footage which has been retained for a longer period of time should require a higher standard of review before access is allowed. Rules for access are provided in Sections 315–324.*

Section 314. Requests for Extended Retention of Archival Recorded Footage Beyond Retention Period.

a. Footage may be retained beyond the retention period designated pursuant to Section 313 only upon specific request of an Operator. Each request shall be submitted in writing upon oath or affirmation of an Operator to [the chief executive officer of the Operating Agency, or his or her designee], and shall include all of the following:

   1. a full and complete statement of the purpose for which the requested Footage is to be retained; and

   2. a detailed description of what is contained in the requested Footage, including details regarding the particular offense or offenses of which the Footage may provide evidence, and the identity or identities, if known, of the person or persons whose image(s) is or are depicted in the Footage.

b. A request submitted under subsection (a) of this Section may be granted if [the chief executive officer of the Operating Agency, or his or her designee] determines, based on all the facts submitted in the request, one of the following:

   1. The purpose for which the Footage will be retained is consistent with the approved purpose of the Public Video Surveillance System as articulated by the [Governing Body] in its Final PVS Impact Report, Section 209, and there is a reasonable suspicion that the Footage in question contains evidence of criminal activity or is relevant to an ongoing investigation or pending criminal trial.

   2. The purpose for which the Footage will be retained is a Secondary Purpose, and there is probable cause to believe that the Footage in question contains evidence of criminal activity or is relevant to an ongoing investigation or pending criminal trial.

c. Footage retained pursuant to a properly granted request under this Section need not be automatically deleted after the expiration of the retention period set under Section 313.

d. If a request for extended retention under Subsection (b) of this Section has been granted, retained Footage may be accessed and used by the Operator and Operating Agency for the uses consistent with the reasons given in support of the retention request only. Access to Footage retained under Subsection (b) of this Section for purposes other than that given in support of the retention request must comply with the requirements for access to archival Footage in Section 316–317.

e. Footage may be retained beyond the retention period in connection with a formal complaint or disciplinary proceeding or investigation against an Operator or other member of the Operating Agency, where there is reason to believe that the Footage in question is relevant to that incident or investigation. Requests for such retention should follow the procedures set forth in Subsections (a) and (b) of this Section.

> ***Legislative Note:*** *Note that requests for extended retention must ultimately come from the Operator, but the showing required to retain the Footage may be based on facts and circumstances disclosed by other governmental agencies. This Section is intended to include requests to retain Footage of critical public infrastructure, such as the Brooklyn Bridge, over an extended period of time. This would enable law enforcement to review such Footage to detect any activities to scout or "case" the location over time as part of a terrorist plot. Such patterns might not become apparent during the pre-archival period of one week.*

Part 2. Access to and Use of Recorded Footage.

Section 315. Access to or Disclosure of Public Video Surveillance Footage and Data to Third Parties Prohibited.

Except as otherwise provided in Sections 320–324 of this [act], the Operator or Operating Agency shall not disclose Footage or other data gathered or compiled by or stored in a Public Video Surveillance System to Third Parties, or provide to or allow Third Parties to access such Footage or data.

> ***Legislative Note:*** *Communities should restrict, to the extent possible, use of public video surveillance data by Third Parties. Especially to the extent the data reveals identifiable individuals, sharing of data without the consent of the individuals severely undermines individuals' confidence in official motives for collecting such information, and further threatens constitutional rights and values. While releasing Footage may be beneficial in some cases, in general disclosures to Third Parties creates increased risk of the information being used for improper and unaccountable purposes. Please see Sections 320–324 for the situations in which disclosure to and access by Third Parties are permissible.*

Section 316. Operating Agency Access to and Use of Recorded Footage for Primary Purpose.

An Operator or Operating Agency may access and use Recorded Footage for purposes consistent with purpose of the System as articulated by the [Governing Body] in its Final PVS Impact Report, Section 209, or in accordance with the order obtained under Section 314. No additional approval is required for such use, once the Footage has been properly retained pursuant to Section 313 or 314.

> ***Legislative Note:*** *This provision applies to all Recorded Footage, regardless of how long it has been retained.*

Section 317. Operating Agency Access to and Use of Recorded Footage for Secondary Purpose.

a. Except as provided in this Section, the Operator or Operating Agency may not access or use Recorded Footage for a Secondary Purpose.

b. *Administrative approval for pre-archival Footage:* Pre-archival Recorded Footage may be accessed and used by the Operator or Operating Agency for a Secondary Purpose upon specific request of an Operator, provided that:

1. Each such request is made in writing upon oath or affirmation of an Operator to [the chief executive officer of the Operating Agency, or his or her designee], and includes all of the following:

   i. a full and complete statement of the facts and circumstances relied on by the applicant to justify his or her belief that such an order should be issued, including: (A) details regarding the particular offense that has been, is being, or is about to be committed; (B) a particular description of the location or locations of such offense; and (C) the identity, if known, or a description of the person(s) believed to be involved in the commission of the offense; and

   ii. a description of the Footage to be accessed or used, including identification of the cameras through which the Footage was obtained, and the time periods for which access is requested.

2. A request submitted under Subsection (b)(1) of this Section may be granted if [the chief executive officer of the Operating Agency, or his or her designee] determines, based on all the facts submitted in the request, all of the following:

   i. there is probable cause to believe that an individual is committing, has committed, or is about to commit an offense carrying a term of imprisonment greater than one year; and

   ii. there is probable cause to believe that evidence of or information about that crime or the individual who committed that crime will be obtained by access to the Footage described in the application.

c. *Court approval for archival Footage:* Archival Recorded Footage may be accessed and used by the Operator or Operating Agency for a Secondary Purpose upon the [Operator, Operating Agency, or district attorney's] application for an order from a court of competent jurisdiction authorizing access to archival Recorded Footage.

1. Each such application must be made in writing upon oath or affirmation of an Operator to [a judge of competent jurisdiction], and shall include all of the following:

   i. a full and complete statement of the facts and circumstances relied on by the applicant to justify his or her belief that such an order should be issued, including: (A) details regarding the particular offense that has been, is being, or is about to be committed; (B) a particular description of the location or locations of such offense;

and (C) the identity, if known, or a description of the of the person(s) believed to be involved in the commission of the offense.

ii. a description of the Footage to be accessed or used, including identification of the cameras through which the Footage was obtained, and the time periods for which access is requested.

2. Upon application made under Subsection (c)(1) of this Section, the judge may enter an order, as requested or modified, authorizing access to archival Recorded Footage within the territorial jurisdiction of the court in which the judge is sitting, if the judge determines, on the basis of the facts submitted by the applicant, all of the following:

   i. there is probable cause to believe that an individual is committing, has committed, or is about to commit an offense carrying a term of imprisonment greater than one year; and

   ii. there is probable cause to believe that evidence of or information about that crime or the individual who committed that crime will be obtained by access to the Footage described in the application.

3. Each order authorizing use of Footage for a Secondary Purpose shall specify all of the following:

   i. a particular description of the Footage to which access is granted, including the location of the camera or of the location depicted in the Footage, and the time when the Footage was Recorded;

   ii. the identity of the person(s), or if their identity is unknown, a description of, the person(s) believed to be involved in the commission of the offense and depicted in the Footage to which access is granted.

d. Footage retained under Section 314 may be accessed and used by the Operator or Operating Agency as part of the investigation and prosecution of the offense under which the request for retention was made.

Legislative Note: *In general, the use Public Video Surveillance Systems should be limited to the purpose for which the System was approved under Article I of this [act]. Therefore, potential use for Secondary Purposes should be paid closer scrutiny. This Section provides different procedures for access to Footage for Secondary Purposes based on whether that Footage is pre-archival or archival. Approval for access to pre-archival Footage need only be sought from an appropriate administrative official, while access to archival Footage requires approval of a judge.*

Subsection (c)(2)(i) of this Section places a limit on use for Secondary Purposes of Footage by requiring that the offense being investigated carry a sentence of more than one year imprisonment. Jurisdictions may use their judgment in altering this limitation to suit their needs, such as by listing the particular offenses or classes of offenses that are appropriate subjects for the use for Secondary Purposes of Footage.

Section 318. Operating Agency Access to and Use of Recorded Footage for Secondary Purposes Under Exigent Circumstances.

a. Upon informal application by the [Attorney General, Chief Deputy Attorney General, a district attorney, or an individual within the Operating Agency authorized by any of the above persons], a [judge of competent jurisdiction] may grant oral approval for access to Recorded Footage for a Secondary Purpose, without an order, if he or she determines all of the following:

   1. There are grounds upon which an order could be issued under this chapter.

   2. There is probable cause to believe that an emergency situation exists.

   3. There is probable cause to believe that a substantial danger to life or limb exists justifying the authorization for immediate access to Recorded Footage before an application for an order could with due diligence be submitted and acted upon.

b. If the person seeking oral approval for access to Recorded Footage for a Secondary Purpose under this Section is unable, after a good faith effort, to contact a [judge of competent jurisdiction], such person may authorize and proceed with the emergency access to Recorded Footage without an order, if he or she determines all of the following:

   1. There are grounds upon which an order could be issued under this chapter.

   2. There is probable cause to believe that an emergency situation exists with respect to the investigation and/or prevention of an offense carrying a term of imprisonment greater than one year.

   3. There is probable cause to believe that a substantial danger to life or limb exists justifying the authorization for immediate access to Recorded Footage before an application for an order could with due diligence be submitted and acted upon.

c. Approval for access to Recorded Footage for a Secondary Purpose under this Section shall be conditioned upon filing with the judge, within 72 hours of the oral approval under Subsection (a) of this Section or a determination under Subsection (b) of this Section, a written application for an order which, if granted consistent with this chapter, shall also

recite the oral approval under Subsection (a) or determination under Subsection (b) and be retroactive to the time of such oral approval or determination.

Legislative Note: *This exception for access to Recorded Footage for Secondary Purposes under exigent circumstances makes no distinction between pre-archival and archival Footage.*

Section 319. Incidental Use of Public Video Surveillance System by Operating Agency.

When using a Public Video Surveillance System for approved purposes, if the Operator observes any activities or events arousing reasonable suspicion of criminal activity, the Operator may use that information for other legitimate law enforcement activities, even those inconsistent with the purposes of the PPVS System.

Section 320. Criminal Defendants.

a. In accordance with [state and federal rules of criminal procedure], defendants in criminal cases may obtain Video Surveillance Footage related to the charges pending against them that is within the government's possession, custody, or control.

b. If Video Surveillance Footage is intended to be used in the prosecution's case in chief in a criminal trial, the criminal defendant shall be provided with all of the following:

   1. copies of all the Footage intended to be used in the prosecution's case in chief at trial. The Footage provided shall include both the particular segments contemplated for use in the case in chief, and all other Footage Recorded by the same camera within 24 hours of the segments intended to be used;

   2. copies of any Automatic Identification or Automatic Tracking orders and their accompanying applications, if any warrants were obtained or applied for; and

   3. access logs [and other relevant data] corresponding with the provided Footage.

c. Footage disclosed to criminal defendants under this Section shall not be disclosed to the public, except to the extent necessary to defend against the criminal charges in the action under which the Footage is disclosed.

Legislative Note: *State and federal procedures and standards for access to Recorded Footage by criminal defendants should be adhered to in providing Video Surveillance Footage to such parties. This Section should not be interpreted to have*

any effect on the government's duty to disclose material, exculpatory evidence to a criminal defendant.

Section 321. Access to Recorded Footage in Civil Suits Between Private Litigants Prohibited.

a. Data collected by Public Video Surveillance Systems shall not be available to the parties or discoverable in civil trials between private litigants, except as provided in Subsection (b) of this Section.

b. Data collected by a Public Video Surveillance System shall be available to a private litigant upon a showing to the presiding judge that such Footage is needed to prevent imminent Harm to life or limb, such as in a proceeding to obtain a restraining order.

Legislative Note: *This Section is not intended to preclude access to video surveillance data in a suit alleging police misconduct, in which the government would typically be a party to the litigation. To the extent that under applicable state laws police misconduct suits would be considered litigation between private litigants, this provision may need to be modified accordingly.*

Section 322. Access to Recorded Footage Under The State [Public Records Act].

Public Video Surveillance Footage and data from a Public Video Surveillance System shall not be considered [public records] for purposes of the [state public records or freedom of information act].

Legislative Note: *Given the potential threats to privacy and other constitutional rights and values posed by wide disclosure of Footage and data collected by Public Video Surveillance Systems, and the expense of reviewing and providing this information, this information should not be available to the public under state public records or freedom of information acts. Other measures, such as publicly accountable approval procedures and audit requirements, reintroduce a measure of public accountability to these Systems.*

Section 323. Access to Recorded Footage by Other Governmental Entities.

a. Except as provided in Subsection (b) of this Section, or as [required by federal law], a governmental authority other than the Operating Agency may not access or use Recorded Footage.

b. A governmental authority other than the Operating Agency for the PVS System may apply for an order authorizing access to Recorded Footage.

   1. Such applications must be made in writing upon oath or affirmation of an Operator to [a judge of competent jurisdiction], and shall include all of the following:

      i. a full and complete statement of the facts and circumstances relied on by the applicant to justify his or her belief that such an order should be issued, including: (A) details regarding the particular offense that has been, is being, or is about to be committed; (B) a particular description of the location or locations of such offense; and (C) the identity, if known, or a description of the of the person(s) believed to be involved in the commission of the offense.

      ii. a description of the Footage to be accessed or used, including identification of the cameras through which the Footage was obtained, and the time periods for which access is requested.

   2. Upon application made under Subsection (b)(1) of this Section, the judge may enter an *ex parte* order, as requested or modified, authorizing access to Recorded Footage within the territorial jurisdiction of the court in which the judge is sitting, if the judge determines, on the basis of the facts submitted by the applicant, all of the following:

      i. there is probable cause to believe that an individual is committing, has committed, or is about to commit an offense carrying a term of imprisonment greater than one year; and

      ii. there is probable cause to believe that evidence of or information about that crime or the individual who committed that crime will be obtained by access to the Footage described in the application.

   3. Each order authorizing access to Recorded Footage under this Section shall specify all of the following:

      i. a particular description of the Footage to which access is granted, including the location of the camera or of the location depicted in the Footage, and the time when the Footage was Recorded; and

      ii. the identity of the person(s), or if their identity is unknown, a description of, the person(s) believed to be involved in the commission of the offense and depicted in the Footage to which access is granted.

Legislative Note: *Note that here, unlike when access to Footage is being requested by the Operating Agency, the distinctions between archival and pre-archival Footage, and use for primary or Secondary Purposes, are irrelevant—all requests for access to Footage are judged by the same standard.*

Section 324. Access to Recorded Footage by Other Governmental Entities Under Exigent Circumstances.

a. Upon informal application by [a designated official in the requesting government agency] of a governmental authority other than the Operating Agency for the PVS System, a [judge of competent jurisdiction] may grant oral approval for access to Recorded Footage, without an order, if he or she determines all of the following:

   1. There are grounds upon which an order could be issued under this chapter.
   2. There is probable cause to believe that an emergency situation exists.
   3. There is probable cause to believe that a substantial danger to life or limb exists justifying the authorization for immediate access to Recorded Footage before an application for an order could with due diligence be submitted and acted upon.

b. If the person seeking oral approval for access to Recorded Footage under this Section is unable, after a good faith effort, to contact a [judge of competent jurisdiction], such person may authorize and proceed with the emergency access to Recorded Footage without an order, if he or she determines all of the following:

   1. There are grounds upon which an order could be issued under this chapter.
   2. There is probable cause to believe that an emergency situation exists with respect to the investigation of an offense the investigation and/or prevention of which is consistent with the purpose of the System as articulated in the Final PVS Impact Report.
   3. There is probable cause to believe that a substantial danger to life or limb exists justifying the authorization for immediate access to Recorded Footage before an application for an order could with due diligence be submitted and acted upon.

c. Approval for access to Recorded Footage under this Section shall be conditioned upon filing with the judge, within 72 hours of the oral approval, a written application for an order which, if granted consistent with this chapter, shall also recite the oral approval under Subsection (a) or determination under Subsection (b) and be retroactive to the time of such oral approval or determination.

Part 3. Integrity and Security of Permanent Public Video Surveillance System and Stored Data.

Section 325. Security Safeguards for Public Video Surveillance System and Stored Data.

a. Access to Recorded data and the physical facilities of a Public Video Surveillance System shall be strictly limited to Operators.

b. The Operating Agency shall implement and maintain reasonable technological security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure of public video surveillance data.

> ***Legislative Note:*** *Technological safeguards can be costly and complicated. We believe, however, that they are necessary to protect against the significant privacy risks that come with implementation of a technologically sophisticated Public Video Surveillance System. Further measures, such as encrypting all data and entrusting the encryption keys to an independent body that releases Recorded data only upon proper authorization from a judge or administrative official, may be required at the enacting body's discretion.*

Section 326. Training for Operators With Access to Public Video Surveillance System.

a. The [Operating Agency] of a Public Video Surveillance System shall provide training for all Operators. Training must cover all the following topics:

   1. the technical operation of the System, including manipulation of the cameras and access to the data storage facilities;
   2. all applicable laws, rules, and policies regarding the System; and
   3. sanctions for Misuse or abuse.

b. Access to a Public Video Surveillance System and its facilities and stored data, including but not limited to control rooms, databases, and cameras, by the Operator and its employees or agents shall be limited to enumerated lists of authorized Operators who have completed the requisite training program described in Subsection (a) of this Section, except where data must be provided to Third Parties as enumerated in Sections 320–324.

Section 327. Record-keeping Requirements for Public Video Surveillance Systems.

Detailed records must be kept regarding the operation of and access to the Public Video Surveillance System, including:

a. an ongoing log of all those who maintain, operate, observe, inspect, or access the Public Video Surveillance System and/or any data or Footage collected by that System, including the purposes of each activity, the names of the individuals engaging in that activity, and the times and dates when such access occurs;

b. an ongoing log of all Recorded Footage, including how long the Footage has been retained, why the Recorded Footage was retained, and copies of any orders for extended retention, if they exist; and

c. an ongoing log of all disclosures of Recorded Footage, including a description of what is contained in the Footage, the names of any parties to which the Footage was disclosed, when the Footage was disclosed, the reasons for disclosure, and copies of any orders for disclosure, if they exist.

> ***Legislative Note:*** *The maintenance of complete and detailed records of all use of the Video Surveillance System is necessary for ongoing review of the effectiveness and appropriateness of the System as a law enforcement tool. In addition, when published as part of an audit under Section 213, this information can provide some of the public accountability normally attained via public records act requests.*

Part 4. Sanctions, Enforcement, Remedies.

Section 328. Administrative Discipline.

a. The Operating Agency shall provide procedures for investigation of and discipline for abuse or Misuse of the Public Video Surveillance System. This shall include a means by which employees of the agency and members of the public may confidentially report a suspected violation of the provisions of this [act].

b. Any employee who is discharged, demoted, suspended, threatened, harassed, or in any other manner discriminated against in the terms and conditions of employment by his or her employer because of lawful acts done by the employee on behalf of his or her employer or others in furtherance of an action under this [act], including investigation for, initiation of, testimony for, or assistance in an action filed or to be filed under this [act], shall be entitled to all relief necessary to make the employee whole.

Section 329. Exclusionary Rule.

a. A criminal defendant in any trial, hearing, or proceeding against him or her may move to suppress the contents of Footage observed or Recorded pursuant to this chapter, or evidence derived therefrom, on any of the following grounds:

   1. The Footage or other information from the Public Video Surveillance System was collected in a manner constituting a substantial violation of a provision of this [act].

   2. The order of authorization or approval under which the Footage was collected is insufficient on its face, such that it would be unreasonable for an Operator to rely on its sufficiency.

   3. The Footage or other information was not collected in conformity with the order of authorization or approval.

b. A motion under Subsection (a) of this Section shall be made, determined, and subject to review in accordance with [state law].

Legislative Note: *In order to be effective, this provision requiring the exclusion of evidence gathered in violation of this act must likely be enacted at the state level. In addition, this Section should reference state statutory provisions regarding the making and adjudicating of motions to suppress.*

Section 330. Private Right of Action.

a. Any person who is:

   1. depicted in Video Surveillance Footage, or described by data attached to Video Surveillance Footage, which is improperly disclosed, accessed, or retained in violation of this [act];

   2. Automatically Tracked in violation of Sections 307, 308, or 309;

   3. Automatically Identified in violation of Sections 302, 303, or 309, including both individuals whose images appear in video Footage on which Automatic Identification is performed, and individuals whose personal information is revealed as a result of Automatic Identification or appended to Video Surveillance Footage;

   4. the subject of Pan, Tilt, or Zoom activity in violation of Section 311; or

   5. publicly but mistakenly identified as appearing in Video Surveillance Footage depicting commission of a criminal act;

may in a civil action recover from the person or entity which engaged in that violation such relief as may be appropriate.

b. In an action under this Section, appropriate relief includes:

   1. such injunctive and other equitable or declaratory relief as may be appropriate;

   2. actual damages but not less than liquidated damages computed at the rate of:

      i. one hundred dollars ($100) a day for each day of violation or one thousand dollars ($1,000), whichever is greater, if defendant's conduct is negligent; or

      ii. five hundred dollars ($500) a day for each day of violation or five thousand dollars ($5,000), whichever is greater, if defendant's conduct is intentional or reckless;

   3. punitive damages, if defendant's conduct was intentional or reckless; and

   4. a reasonable attorney's fee and other litigation costs reasonably incurred.

c. A good faith reliance on a court warrant or order, or administrative approval under this [act] is a complete defense against any civil or criminal action brought under this chapter or any other law.

d. A civil action under this Section may not be commenced later than two years after the date upon which the claimant first has a reasonable opportunity to discover the alleged violation.

Legislative Note: *This Section provides relief to individuals who have been Harmed by violation of the use restrictions under Article 3 of this [act]. However, claims for violations of Article 2 of this [act] having to do with procedures for implementation may be made in the same action as claims for violations under this Article, although the remedies for such violations are different. Furthermore, evidence of violations of Article 2 of this [act] may in some cases be relevant to claims under this Article, as where, for example, the stated purpose of the System is relevant to whether a violation has occurred. Actions under this Section may be maintained against individual Operators or the Operating Agency.*

Section 331. Enforcement by State Attorney General.

a. The state Attorney General or equivalent state review panel shall be empowered to investigate and review failures to comply with the provisions of this Article, and to issue orders for compliance.

b. Upon a finding of a pattern or practice of violations of this Article, the state may withhold funds from the Operating Agency until the Attorney General is satisfied that a full investigation has been made and steps have been taken by the Operating Agency to reduce the incidence of violation.

Part 5. Other.

Section 332. Public Notice of Public Video Surveillance.

a. Jurisdictions employing a Public Video Surveillance System must post notices in locations subject to public video surveillance that state, in clear language, that such location is subject to Observation and, if applicable, recording, by a Public Video Surveillance System.

b. Notices posted pursuant to Subsection (a) shall be posted within 7 days of the initiation of the System, and shall be in clear language, large type, and in a conspicuous location plainly visible to persons present in the surveilled area. Notices need not, however, disclose the precise location of the camera(s).

c. If the Public Video Surveillance System is temporary and installed pursuant to a court order obtained under Section 210, notices of surveillance, including a description of the locations surveilled, must be published in local newspapers or through electronic means according to applicable pubic notice regulations no later than 30 days after (1) termination of the surveillance or (2) a determination that such disclosure will no longer jeopardize the investigation or reasonably related investigations. Notices published pursuant to this Subsection must be published for no fewer than 7 consecutive days.

> ***Legislative Note:*** *To permit informed choices and provide accountability, those subject to video surveillance should be made aware of it. While for security as well as aesthetic and social reasons, many communities may want to hide or disguise the actual cameras, there is generally no basis for hiding the fact that an area is under government surveillance. These notifications need not be intrusive, but should nevertheless be visible. We recommend that authorities place small placards in the surveilled area noting the presence of video surveillance and providing contact information for those wishing more information on the camera System. Subsection (c) intends to provide an exception for purposes which require a measure of secrecy at their Installation.*

Section 333. Privately Collected Public Video Surveillance Data.

The government shall not use privately collected video surveillance of public places with such regularity as to effectively circumvent the provisions of this act. If the Operating Agency obtains Footage of public places from private cameras, the use and retention of such Footage shall be subject to all the requirements of Article 3 of this Act, to the same extent as if the Footage had been obtained from government owned and operated cameras.




The Constitution Project is an independent think tank that promotes and defends constitutional safeguards. The Project creates coalitions of respected leaders of all political stripes who issue consensus recommendations for policy reforms, and conducts strategic public education campaigns to transform this consensus into sound public policy.

The Constitution Project
1025 Vermont Avenue, NW
Third Floor
Washington, DC 20005

(202) 580-6920 (tel)
(202) 580-6929 (fax)

info@constitutionproject.org
www.constitutionproject.org