Prepared Statement
Deirdre K. Mulligan
Clinical Professor of Law
Director, Samuelson Law, Technology & Public Policy Clinic
UC Berkeley School of Law (Boalt Hall)

Before the
Department of Homeland Security
Data Privacy and Integrity Advisory Committee

June 7, 2006

In Defense of Public Spaces

I. Introduction and Summary of Remarks

Thank you for the opportunity to present my views on "Expectations of Privacy in Public Spaces" to the Data Privacy and Integrity Advisory Committee. My remarks today offer three observations and three sets of recommendations.

First, public spaces support functions that democracies care about. They are the venues in which citizens (and non-citizens) exercise speech and associational rights. They are the locus of the unplanned interactions between the citizenry that force public discourse and debate. They are the only space in which people who lack private places may legitimately be. From the political speaker on her soapbox, to the religious proselytizer going door-to-door, to the demonstrator on the sidewalk, each relies on the availability and particular qualities of public spaces. Public spaces must be traversed to arrive at private places. Thus an individual visiting her doctor, lawyer, religious institution, or political organization will likely approach and enter it from a public space. The significant role of public places in deliberative democracy and in individuals' daily lives, require us—and I do mean "us" as this rightly should be a national conversation—to consider the potential consequences of introducing pervasive visual surveillance. We must ask whether individuals, unable to assess whether, when, and for what purpose they are being observed by the state, will alter their use of public places. For if these public places become safe but not free, they will likely prove incapable of sustaining the exchanges and activities for which we've jealously protected them.

Second, we are at a constitutional moment with insufficient guidance from constitutional courts. Across the country, in large urban as well as small rural areas, often supported by DHS grants, surveillance systems are being deployed. Unsurprisingly the question of what limits the constitution establishes on government use of public video surveillance systems to watch all individuals who pass through a public space, most of whom are suspected of no wrong doing, has not been squarely presented to the courts. Never before has a surveillance system of this breadth and coverage been deployed.

Third, while the lack of direct case law defining the privacy and other interests in such a scheme is understandable given the contrasting speed of technological advancement and the deliberate, unhurried pace of legal decisions, the lack of public oversight and debate, about whether and under what circumstances and with what checks

and balances such systems are appropriate, is not. The visual surveillance systems being pursued by various localities will monitor large swaths of the public, the majority of whom are suspected of no wrongdoing. The systems have the potential to monitor and record individual and group activities on an unprecedented scale. In many respects these systems turn the Fourth Amendment on its head. They search each and every individual in the camera's gaze based on no particularized suspicion of wrongdoing. The searches are unobtrusive, often invisible, providing citizens little to no opportunity to monitor governments monitoring of citizens. Given the potential of these systems to fundamentally alter the balance of power between citizens and the government and erode the utility of public spaces for democratically significant activities, the lack of clarity about what the constitution requires or limits should not shield these systems from critical review and regulation. Rather than waiting for the courts to tell us what the Constitution demands, we should be asking what a free and open society requires. If we fail to engage in reasoned public inquiry and debate about the benefits and costs—in terms of dollars and democratic values—of public surveillance systems we may irresponsibly invest public funds, needlessly erode the privacy and freedom quintessential to public places, and miss the chance to conform the technologies and policies of surveillance systems—where society decides they are warranted—to align with democratic values.

Based on these observations I offer three sets of recommendations to the Committee. The first set of recommendations the Committee is uniquely situated to urge DHS to act upon. The second two I offer to the Committee for its consideration. This Committee has proven itself willing to provide forward-looking, expansive, and controversial advice. While you may be less able to prompt swift action on the later recommendations, I have no doubt that if they were adopted by this Committee the recommendations would command serious consideration. It is with this hope that I offer them.

First, the Department of Homeland Security should require potential recipients of DHS grants to conduct a Privacy Impact Assessment of video surveillance systems as a condition of receiving funds. As this Committee is well aware, the Department of Homeland Security is required to conduct privacy impact assessments to ensure that technology it uses respects certain privacy interests. It would be fully consistent with the spirit of the E-government Act to require grantees to engage in privacy impact assessments before installing massive public surveillance systems.

Second, public oversight and accountability must be built into the decision about where and whether to install public surveillance systems. Toward this end, the Privacy and Integrity Advisory Board should recommend that the initial award of a DHS grant for the establishment of public surveillance systems be made with public input and that localities requesting DHS monies for the establishment of public surveillance systems be required to engage the public in a formal process to consider the costs and benefits, both economic and social, of the proposed installation, and established technical limitations, policies and procedures to govern the system and guard against misuse.

Third, federal law must be updated to address the use of advanced visual surveillance technology by the government. As then Associate Justice Rehnquist wrote in a 1974 law review article, "In Hitler's Germany and Stalin's Russia, there was very efficient law enforcement, there was very little privacy, and the winds of freedom did not blow."[1]There is no end in sight in the war on terror. Technological advances that will enable the government to engage in increasingly invisible yet invasive, and certainly oppressive if not carefully controlled, surveillance are on the horizon. We may as a society determine that our safety and freedom require that some public spaces be subject to enhanced visual surveillance systems. Clearly such a decision should be the product of a robust debate and such systems should be accompanied by checks and balances that preserve the freedoms and liberties of all those whose lives will be subject to surveillance. To date Congress has been largely silent on our federally subsidized slide into surveillance.[2] Given the important role statutory privacy laws play in governing electronic surveillance in other forms—providing more detailed rights and obligations than case law typically does—and the federal government's role in funding the creation of a distributed public surveillance infrastructure it is time for Congress to establish a federal framework to govern public visual surveillance systems.

Sliding towards surveillance is unacceptable in a democratic civil society. This Committee is well positioned to call for reforms that will ensure that public surveillance systems funded by federal tax dollars provide for our security, protect our liberties, and are economically sound. I urge you to do so.

II. The Town Square Under Surveillance – Publicly Funded but not Publicly Accountable

Surveillance cameras long ago became a permanent part of the American landscape. At banks, convenience stores, apartment buildings and shopping malls, we have grown accustomed to being under the video camera's unblinking gaze.

But in the public arena –the steps of City Hall, municipal parks, the town commons – surveillance cameras have been slower to proliferate. Since the terrorist

---

[1] William Rehnquist, Is An Expanded Right of Privacy Consistent With Fair and Effective Law Enforcement? Or: Privacy You've Come a Long Way, Baby, 31 KAN. L. REV. 1, 23.

[2] On Dec. 15, 2005, The House Committee on Homeland Security, Subcommittee on Management Integration and Oversight, held a hearing on the Integrated Surveillance Intelligence System (ISIS) on the U.S.-Mexico border. The hearing was titled "Mismanagement of the Border Surveillance System and Lessons for the New Secure Border Initiative." Richard L. Skinner, Inspector General of DHS testified that the remote video surveillance system already in place on the U.S.-Mexico border was ineffective and had fallen short of expectations. Skinner testimony available online at http://hsc.house.gov/files/Testimony%20Skinner.pdf.

On March 22, 2002, the House Committee on Government Reform held hearings on the use of video surveillance in Washington, D.C. In June 2003, the General Accounting office released a report on video surveillance systems installed by the U.S. Park Police and the Metropolitan Police Department, noting that the Constitution Project found the police department's regulations for the use of CCTV "lacked clarity and specificity in some areas, such as training of CCTV operators." Report available online at http://www.gao.gov/new.items/d03748.pdf.

attacks of September 11, that has changed rapidly, and for some obvious and understandable reasons.[3] But this explosion in public surveillance cameras has been rapid, often ill advised and extremely uneven.[4]

It has also been largely funded by the Department of Homeland Security. Through millions of dollars in grants to cities and towns across the country, the Department of Homeland security is helping to build a massive, nationwide surveillance infrastructure that is permanently changing the nature of our public spaces, and in the process threatening core constitutional liberties. Yet there has been virtually no serious or methodical consideration given to the civil-liberties impact, not to mention the economic rationale, of this emerging federally funded surveillance network. This is dangerous.

Without appropriate, sensible safeguards, not only our constitutionally protected liberties are at risk, but also the very security, which these cameras purport to enhance. Permanent surveillance systems have not proven cost-effective (or effective generally) at cutting down on crime, or even aiding in the prosecution of crime. There are many other policing options, but the allure of surveillance cameras can be quite powerful, particularly when federal largesse is involved. But in many instances, cameras are unlikely to meet communities' economic needs, social norms or privacy concerns.

The problem is that nobody is even asking these questions.

Does Dillingham, Alaska (population 2,400) need 80 police surveillance cameras – four times the number of police surveillance cameras in the District of Columbia – to protect the United States against terrorist attack? They may. But the residents of Dillingham were never afforded an opportunity to ask that question before their City Hall was equipped, entirely with DHS grant money, with a cluster of eight surveillance cameras giving authorities a panoramic view of the entire town center. [5]

---

[3]While there are many conflicting reports, many studies strongly suggest that surveillance cameras are, in the long run, of very little assistance in deterring ordinary crime, much less terrorism. *See*, *e.g.*, "The impact of CCTV: fourteen case studies" (2005), a report prepared for the British Home Office, available at www.homeoffice.gov.uk/rds/pdfs05/rdsolr1505.pdf (noting, at p. 1, that while some local CCTV systems appeared to contribute to crime reduction, "it must be borne in mind that there were a limited number of instances where the changes were statistically significant and in fact, all changes might be attributed to chance rather than to any characteristic of the system."); Jason Ditton, Crime and the City: Public Attitudes toward Open-Street CCTV in Glasgow, 40 BRIT. J. CRIMINOL. 692-709 (2000) (recorded crime increased by 9% in Glasgow after CCTV was installed); Jennifer M. Granholm, Video Surveillance on Public Streets: the Constitutionality of Invisible Citizen Searches, 64 U. Det. L. Rev. 687, 688 (1987) (Hoboken, N.J., Charleston, West Virginia and Miami Beach curtailed, cancelled or modified surveillance programs after finding them ineffective).

[4] For discussion on the growth of surveillance cameras, *see*, *e.g.*, Clive Norris, Mike McCahill and David Wood, "The Growth of CCTV: a global perspective on the international diffusion of video surveillance in publicly accessible space," 2 SURVEILLANCE AND SOCIETY 2/3, 110-135 (2004) (annual revenues from the sale of surveillance cameras tripled from $282 million in 1990 to more than $1 billion in 2000; industry analysis predicted a five-fold increase in revenues within one year after the 2001 terrorist attacks).

[5] *See* Tomas Alex Tizon, "80 Eyes on 2,400 People; If terrorists come to tiny Dillingham, Alaska, security cameras will be ready. But privacy concerns have residents up in arms." L.A. TIMES, March 28, 2006 at A1.

How will those cameras affect the civil liberties of Dillingham residents? The question has apparently gone unasked in any formal way.

Does rural Bellows Falls, Vermont (population 3,000), more than 100 miles from any major urban area, need 18 police cameras to thwart Al Qaeda? Again, they may. But the question was never asked in any publicly accountable way before police installed, again with DHS money, the cameras in the town center. [6]

The Pittsburg, California police department installed a network of 11 cameras last year. Newnan, Georgia (population 22,000) has 20 police cameras.[7]

The same story is playing out from coast to coast, usually with significant help from DHS grants.[8] Towns like Ridgely, Maryland; Galax, Virginia; and San Luis Obispo, California, along with cities like Fresno and Dallas have rushed to equip their town centers – their public spaces – with state-of-the-art surveillance technology.[9]

In 2004, DHS funds bought $193 million worth of surveillance cameras.[10] While there does not appear to be any publicly available list of the communities where DHS money has provided surveillance cameras, it is clear from news reports and DHS budget figures that this number is only likely to rise, and that these hundreds of millions of dollars are being funneled –without oversight – to local communities to install surveillance systems as a small handful of local leaders, mostly police, see fit.[11]

The upshot of all this is that surveillance cameras are changing the very notion of what we mean by "public space." It is now possible for the authorities, with the simple flick of a switch, to see what you read – to read what you read – as you sit on a bench on the National Mall. Before long, it will be technologically possible for those authorities o capture a photograph of your face, store it in a database for future use, and compare it against thousands if not millions of other facial photographs. In public spaces in American towns and cities, the general public is now subject to 24-hour surveillance that is capable of seeing things a human being cannot. To date the public remains largely unaware of the extent of surveillance. As knowledge of public surveillance systems grows, the systems will constrain people – criminals and law-abiding citizens alike.

But while studies have shown that the criminals may simply move elsewhere to commit their crimes, away from the camera's never-ending gaze, the activities for which

---

[6] *See* David A. Fahrenthold, "Federal Grants Bring Surveillance Cameras to Small Towns; Village in Vermont Has Almost as Many as D.C.," WASH. POST, January 19, 2006 at A1

[7] *Id*.

[8] *See* "Spotlight on Surveillance, May 2005: More Cities Deploy Camera Surveilleance Systems with Federal Grant money," a report by the Electronic Privacy Information Center, *available at* http://www.epic.org/privacy/surveillance/spotlight/0505/.

[9] *See* David A. Fahrenthold, *supra*, note 4.

[10] Audrey Hudson, Counterterror grants fund city cameras, data mining, WASH. TIMES, May 19, 2005 quoting DHS spokesman Marc Short.

[11] See, e.g., "Spotlight on Surveillance," *supra*, note 7; Audrey Hudson, Counterterror grants fund city cameras, data mining, WASH. TIMES, May 19, 2005.

"place" matters can't simply be relocated. The National Mall, the town square, the steps of City Hall – our democracy cannot survive without these vibrant public spaces. For as long as Western democracies have existed, what political philosopher Jurgen Habermas called the Public Sphere has been an essential focal point of the kind of education, agitation, cultural exchange and simple serendipitous encounters that make democratic self-governance possible.

Our republic requires informed citizens. It requires citizens who are not afraid to speak their minds, and who are free to trade ideas in the public square. It requires the free-flow of ideas and information. All of these things are critically damaged when the physical space that allows for this activity – the public sphere – is dominated by pervasive, 24-hour government surveillance.

These are unique spaces – the physical and geographical manifestations of our First Amendment right to speak our minds, to seek redress from our elected leaders, to gather and share ideas. They are precious cornerstones of our democracy. They are neither fungible nor replaceable.

But they *can* be sanitized. Scrubbed clean of the boisterous cacophony that makes our democracy vibrant, accountable and secure.

In short, if we continue to believe in the importance of these public places because of the foundational role they play in supporting our republican democracy we must consider the effects of the introduction of public surveillance systems on their ability to function as we believe they ought. Extraordinary care must be taken before deciding to put these American spaces in jeopardy.

There is an undeniable need to bolster our security, but that need is not so great that it should overcome our ability to make these decisions with at least a modicum of democratic – small "d" – discussion, after a conversation about what we inevitably give up when we decide to increase our sense of security.

There is a delicate balance to be struck here, and many difficult questions to solve – the kind of questions that in the best American tradition have always been solved with the full benefit of public debate and argument and even protest in the very public places that today are quietly being radically altered.

Because the federal government is playing such a large role in the growth of these publicly funded cameras, the federal government should also bear the burden of ensuring that the money is not wasted; that it is spent on programs that are deemed appropriate after full public input; that it is not abused; that it is consistent with our commitment to a free and open society.

To date, it is clear this is not happening.

A."Public" and "Private" are not Mutually Exclusive Concepts

We all expect some degree of privacy, even in public. Surveillance cameras, particularly the newest and most powerful ones, disrupt this expectation in myriad ways. We don't expect our every move to be filmed, recorded, databased somewhere – maybe many miles or hundreds of miles away – for instant recall at any point in the future. We don't expect to be the subject of close-up photographs when the photographer is utterly invisible. We don't expect anyone to be able to read what we are reading, or watch the numbers we dial on our cell phones or follow us as we walk from street to square to shopping mall.

Surveillance cameras destroy the sense of mutuality that normally inheres in observation. That is to say that normally when we are watched, we can watch back: We can size up our observer, see where he is, and evaluate a potential threat. With surveillance cameras, the watching becomes an inherently imbalanced power arrangement. The government agent, miles away in a control room, completely controls the observation. The subject has no way of even knowing he is being watched. The subject – you, me, anyone in the public sphere, is in many ways a specimen.

Cameras can now see in the pitchest dark, without giving the slightest clue that they are observing and recording. Thermal imaging devices can in some senses see through walls. Pan, tilt and zoom functions allow cameras many hundreds of yards away to see – and to record – the minutest details.

Surveillance cameras also destroy the physical and temporal boundaries that traditionally govern our conception of public space. When we walk across Main Street, we expect our actions to be fleeting – that is, we expect that our actions are not permanently recorded. This temporal limitation coincides with our understanding that the physical space of public areas is limited – that when I travel across Main Street and into an alleyway or the portal of a large building, I have moved from an area of low privacy expectations (Main Street) and into one of higher privacy expectations (the alleyway). Modern surveillance cameras, with the ability to pan, tilt and zoom, treat all of these spaces equally – everyone is subject to constant surveillance and constant recording whether walking across Main Street, walking through an alleyway or ducking into the lobby of a bank.

The 19th century British philosopher Jeremy Bentham proposed a structure he called the panopticon – Latin for "all seeing." From within a tower in the center of the panopticon, authorities could watch every move of the inmates in cells, which were all attached to the central tower.

The power of the structure was that authorities could see the prisoners but the prisoners could never see the authorities, and so the prisoners could never know whether they were being watched. The very possibility that the authorities could be watching was to be a deterrent to bad behavior.

Uncertainty is a great inhibiting force. It is, to use the contemporary military argot, a substantial "force multiplier" – far fewer guards are needed to enforce behavioral norms.

Bentham's idea was picked up by 20th century philosophers, notably Michel Foucault. These thinkers noted that the power of surveillance rises sharply with each new leap in technology, and that particularly in totalitarian regimes, the panopticon concept in some ways came to fruition on a broad, society-wide scale as a means to control entire populations.

It would be hyperbole, as yet, to say that we are creating a modern-day panopticon in the American town square. But there is little doubt we are headed that direction, and quickly. It is clear that surveillance cameras create a chilling effect – sometimes on crime, but just as often on completely lawful activity. They create the sense of being in a prison cell, of being overseen by unseen – and unsee-able – forces.

The conservative New York Times columnist and former Nixon speechwriter William Safire put the danger of this new technology succinctly when he wrote: "To be watched at all times, especially when doing nothing seriously wrong, is to be afflicted with a creepy feeling... It is the pervasive, inescapable feeling of being unfree."[12]

As I will describe in more detail below, courts have generally held that people have no expectation of privacy in "public" spaces, and thus no Fourth Amendment protection against surveillance cameras. But the vast majority of these decisions came before advances in surveillance technology allowed law enforcement to view things that any reasonable person would expect to remain private, particularly with no human presence nearby. When these decisions were made, the capacity of government to monitor the movements of a great portion of the public existed almost entirely in the realm of science fiction. Today, that capacity is real.

Just for one hypothetical example: reading material. Surveillance cameras can achieve the effect of having a police officer standing over the shoulder of someone reading a book, or a political pamphlet, in a city park – or for that matter in their own apartment. The difference is, there is no officer actually there. If there were, the person reading this material would clearly have no expectation of privacy, if they were reading in a park. If they were reading in their own apartment, the story might be different.[13] But either way, as I will explore in more depth below, the right to privacy protects "people, not places," as the Supreme Court held in *Katz v. United States*[14], and therefore is portable.

Clearly, not all "public" space is the same, and the law is slowly evolving to reflect that fact. Courts have recognized that we simply cannot always have to assume

---

[12] William Safire, The Great Unwatched, N.Y. TIMES, Feb. 18, 2002 at A15.
[13] *See*, *e.g.*, *NAACP v. Alabama*, 357 U.S. 449 (holding that a court order requiring the disclosure of membership lists violated First Amendment free association principles).
[14] 389 U.S. 347, 351 (1967).

that we are being watched[15], and that there is a difference between targeted surveillance of a single person or a group of people and broad, sweeping surveillance which to some degree assumes the guilt of everyone within the camera's gaze. The latter type of search, when it is accompanied by a seizure, has often been struck down for violating the Fourth Amendment protection against unreasonable searches.[16] It is well settled that, barring exigent circumstances, a generalized law enforcement urgency cannot justify warrantless searches that conclude in seizures,[17],[18] though there are exceptions, such as drunk-driving checkpoints.[19]

The cases in this area may be distinguishable from a search involving a surveillance camera, because a surveillance camera search might not involve any kind of seizure. But there is some support in Supreme Court case law for the notion that a "search" within the meaning of the Fourth Amendment can be invalid, even absent a "seizure," when technology allows government agents to see things they would not be able to see without the assistance of technology.[20]

As technology makes invasions easier in public spaces, the law will keep pace. But that may take years. The law can take decades to catch up with social mores and standards. Until then, it is essential that the public at least have a say in how this technology changes their lives.

B. How Effective Is Permanent Video Surveillance?

Technological developments in recent years have made it possible for law enforcement to do things – many of them valuable – that were unimaginable even 30 years ago. We are all familiar with high-profile examples of video recordings playing

---

[15] *See*, *e.g.*, *U.S. v. Bruneau*, 594 F.2d 1190, 1196 (8th Cir., 1979) (noting, without deciding the issue, the "persuasive" argument that a police tracking device implicates the Fourth Amendment even in "public" spaces because it "does more than facilitate visual observation: it denies one the opportunity to perceive and perhaps lose his follower; it allows for continual observation over long periods of time; it continues to monitor location when the device enters private property (an area which is off-limits to law enforcement personnel); and it creates the likely possibility that law enforcement personnel will be privy to information exceeding that necessary to trace the crime at hand").

[16] See, e.g., *Torres v. Puerto Rico*, 442 U.S. 465 (1979) (search of luggage without a warrant or probable cause violated Fourth Amendment despite Puerto Rican statute purporting to authorize police to search the luggage of anyone entering from the United States).

[17] *See*, *e.g.*, *Almeida-Sanchez v. United States*, 413 U.S. 266 **(**1973) (warrantless search of defendant's vehicle by roving patrol some 20 miles north of the Mexican border violated protection against unreasonable searches).

[18] Narrow exceptions have been carved out for airport screening searches; border searches and magnetometers in many public buildings.

[19] *Michigan Dep't of State Police v. Sitz*, 496 U.S. 444 (1990) (holding that stopping motorists at highway sobriety checkpoints does not violate the Fourth Amendment because the state interest in preventing drunk driving outweighs the intrusion of the stop on individual rights).

[20] See *U.S. v. Karo*, 468 U.S. 705, 714 (1984) ("The monitoring of a beeper in a private residence, a location not open to visual surveillance, violates the Fourth Amendment rights of those who have a justifiable interest in the privacy of the residence").

some role in the apprehension of criminal suspects. But the extent to which surveillance can actually "break" a case remains doubtful. While the surveillance photographs of the London Underground bombing suspects made worldwide news, and it was surely impressive that such footage could so quickly be located and broadcast, the importance of those images to the police investigation does not seem to have been critically important.[21]

It is easy to overestimate the effectiveness of this technology. A handful of high-profile examples do not necessarily justify pervasive police surveillance. A number of studies, along with the anecdotal experience of cities that have tried surveillance have shown that cameras – particularly cameras alone, without any other changes in police tactics – do very little to deter crime, and are even of questionable value in bringing criminals to justice after the fact.[22]

While many cities and towns rush to embrace surveillance technology, a growing number have rejected it as ineffective, overly obtrusive or both.

Early experiments with permanent video surveillance in Hoboken, N.J., Mount Vernon, N.Y., Miami, Fla., Charleston, S.C. and Detroit Mich. were dropped because they were not cost effective.[23] New York City officials dismantled a Times Square surveillance system when the cameras produced fewer than 10 arrests after 22 months.[24]The failure of these experiments in permanent video surveillance systems may be attributed in part to the primitive technology used. But there are also more recent examples of communities rejecting video surveillance: Oakland officials twice considered and rejected proposals for city-run camera networks. Police concluded that it was valuable to invest in officers on the streets rather than relying on video.[25]

In 2003, two years after Tampa became the first U.S. city to use facial-recognition software, city officials abandoned the program after it yielded no arrests.[26] Tampa police spokesman Joe Durkin told the *St. Petersburg Times* that he didn't "consider it a failure…You are always looking for new and efficient ways to produce the best service to the community. There's going to be ups and downs."[27]

Also in Florida, Seminole County turned off traffic surveillance cameras after public officials expressed concerns that there were no guidelines for ensuring the system

---

[21] . *See* Report of the Official Account of the Bombings in London on 7th July 2005*, available* at http://news.bbc.co.uk/2/shared/bsp/hi/pdfs/11_05_06_narrative.pdf, John Schwartz, Cameras in Britain Record The Criminal and the Banal, N.Y. TIMES, July 23, 2005 at A7

[22] See note 3, *supra*.

[23] Quentin Burrows, Scowl Because You're on Candid Camera: Privacy and Video Surviellance, 31 Val. U. L. Rev. 1079, 1103 (1997); Gary C. Robb, Police Use of CCTV Surveillance: Constitutional Implications and Proposed Legislation 13 U. MICH. J.L. REFORM 571; Maureen O'Donnell, Cameras Around Every Corner, Sun-Times (Chicago), Feb. 18, 1996, at 1.

[24] *Id*.

[25]Thaai Walker, Change of Mind on Oakland Street Cameras Police chief now wants them for traffic only, S.F. CHRONICLE, Sept. 12, 1997 at A21.

[26] Brady Dennis, Ybor cameras won't seek what they never found, St. Petersburg Times, Aug. 20, 2003 at 1A.

[27] *Id*.

would not be abused.[28] Dade County abandoned its surveillance program in 1984, two years after starting it, when the program yielded no arrests.[29]

Large cities around the country have erected elaborate, state-of-the-art surveillance systems, often with little oversight or public input. The U.S. Park Police in Washington, D.C. installed sophisticated surveillance cameras on the National Mall without notifying the public, while the city's police department has installed 19 cameras in commercial districts and other tourist hot spots—also without public notice. Police have agreed to use the cameras only during mass demonstrations and civic emergencies and not to arbitrarily monitor anyone because of race or gender.[30]The District of Columbia's city council passed regulations calling for the cameras to be used only to monitor traffic, large demonstrations and city emergencies. The regulations also say that the cameras can be installed only in public spaces where people would have a reasonable expectation of being videotaped, and they prohibit police from using the devices to watch for ordinary street crime.[31] The police are also required to give community updates about the surveillance system, and requiring routine audits of the police department's use of system.[32] The police chief is required to provide public notice of the police department's intention to deploy any new cameras, and the public notice must include the CCTV system's general capabilities and viewing area, though it does not have to mention the precise location of a new camera.[33] The regulations also require a 30-day public comment period.[34] These strictures apply only to the city's police department, not the federally run cameras on the National Mall.

Unfortunately, these basic restrictions are among the most comprehensive of any municipal surveillance systems around the country.

The next wave in public surveillance technology – the combination of private and public surveillance systems to create a seamless surveillance "blanket" over broad swaths of the public sphere – is already underway in Fresno, California.

City officials plan to merge the city's public and private surveillance systems, allowing police and police dispatchers to view private security cameras through the Internet.[35] The city plans to appropriate more than $1 million for the program, which is also being funded by a DHS grant.[36]The city has no regulations for ensuring that the

---

[28] Robert Perez, County to Turn Off Roadside Cameras, Orlando Sentinel, June 19, 1996 at A1.
[29] Raymond Surette, Video Street Patrol: Media Technology and Street Crime, 13 J. POLICE SCI. & ADMIN. 78, 78 n. 1
[30] D.C. Mun. Regs. tit. 24 §§2505.3-2505.4; *see also* David Fahrenthold, supra note 4.
[31] D.C. Mun. Regs. tit. 24 §§2505.3-2505.4; *see also* Eric M. Weiss, D.C. Might Add Cameras for Police; London Bombings Renew Debate, WASH. POST, July 14, 2005 at B1.
[32] *D.C. Mun. Regs. tit. 24, §2502.1-2502.3.*
[33] D.C. Mun. Regs. tit. 24, § 2502.2
[34] *Id*. §2502.3
[35] Denny Boyles, ACLU irked by Freson police proposal to double cameras, Fresno Bee, March 22, 2006 At A1
[36] The Fresno police department has proposed some guidelines for the surveillance system, but the guidelines include no enforcement mechanisms, no external oversight, and no publicly accountable

system is not abused, and without substantial community input.[37] Fresno police officials have said they plan to double the 121 cameras already in place on public property.

There is little indication that municipalities that have installed video surveillance systems are making any effort to notify the public of such plans, nor is there any indication that towns and cities have enacted procedures to measure their effectiveness. A 2001 survey conducted by the International Association of Chiefs of Police of more than 200 law enforcement agencies found that 96 percent of responding agencies had no way of evaluating whether surveillance systems helped reduce crime.[38]

Perhaps more worrisome is the evident lack of training for officers or civilian staff who operate these systems. The same report found that 54 percent of responding agencies provided no formal training in how to use CCTV systems.[39]

Control over access to video footage is another area of pressing concern. Without strict control over access, surveillance cameras could even compound the harmful effects of crime. For example, if a surveillance camera captured a rape, who will guarantee that footage does not end up on the Internet?

This is not to say that surveillance cameras cannot be valuable in solving crimes. But without strict protocols as to who has access to footage – and when – the potential for abuse grows with each new camera installed. Responsible law enforcement agencies with sufficient resources may draw up their own protocols. Those protocols may be sufficient. But when faced with the prospect of serious constitutional violations, "may" should not be sufficient. Outside agencies – publicly accountable agencies – must have some say in how surveillance cameras are installed, what they can record and how that data can be used.

C. The Potential for Abuse

While the value to law enforcement of round-the-clock surveillance may be questionable, the potential for abuse is not. As towns and cities across the country buy and install comprehensive surveillance systems without oversight or public notice, a few examples of such abuses have recently come to light.

In the spring of 2004, New York City police department surveillance cameras captured the suicide of a man who shot himself in the head in the lobby of a Bronx housing project. Footage of the 22-year-old man's death ended up on the Internet, where it was visible to millions.[40] The video apparently ended up on the Web after a police

---

methods for preventing violations. *See* Mike Rhodes, This Area is Under Surveillance, Community Alliance newspaper, available at http://www.indybay.org/news/2006/05/1825069.php

[37] *Id*.

[38] *See* "The Use of CCTV/Video Cameras in Law Enforcement," *available at* www.iacp.org/documents/pdfs/Publications/UseofCCTV%2Epdf

[39] *Id*. at p. 8.

[40] Shaila K. Dewan, "Video of Suicide in Bronx Appears on Shock Web Site," N.Y. TIMES, April 1, 2004 at B3.

officer emailed the footage to a friend, setting of a chain of emails that ended with the website.[41]

In the UK, where state surveillance is much more prevalent than in the U.S. (and where protections against state intrusions on the individual generally much weaker), a recent example of abuse came in December, when two municipal workers were sentenced for using surveillance cameras to voyeuristically spy on a 37-year-old woman's apartment, filming her undressing and in intimate moments with a boyfriend.[42]

University of Nevada at Reno officials installed a hidden camera outside the office of a controversial professor. The university claimed the camera was installed to protect the professor because of recent slurs directed at him; the professor claimed he was being monitored because he was a whistleblower.[43]

Last year, New York City resident Jeffrey Rosen filed a formal complaint in December with the city's police department after officers filmed him, at night, on the terrace of his Second Avenue penthouse. Police were able to do this from a $9.8 million helicopter with cameras so powerful they can read a license plate 1,000 feet away. The cameras also have thermal imaging equipment that allowed police to observe – and record – nearly four minutes of intimate relations between Rosen and a woman.[44]

Under existing jurisprudence, it might be said that this man was in a "public space" – he was, after all, in open air and could conceivably be observed by others. But only the oddest definition of "public space" could encompass an unlit, private terrace, in the middle of the night. Even in Manhattan, where rooftop binoculars and telescopes can reveal the most intimate moments *inside* apartments or in the open air, the expectation of privacy outside an apartment, completely veiled in dark, is close to absolute.

Courts to date have not to date broadly recognized such distinctions. There is the possibility, if not the probability, that that will change in coming years.

III. Constitutional Issues

Video surveillance implicates a host of constitutional concerns, the most serious of which stem from the First and Fourth Amendments. The Supreme Court has never addressed the question of whether a massive and all-encompassing surveillance system passes constitutional muster. But the court has looked at mass, warrantless searches and has concluded that some types violate the Fourth Amendment, while some do not.[45] With the principles the Court has articulated to date, it seems quite probable that the court would find that mass surveillance runs astray of long-accepted constitutional privacy

[41] Murray Weiss, "Bx. Cop Caught in 'Net – Suicide-Video Scandal," N.Y. POST, June 22, 2004 at 25.
[42] Brian Roberts, "CCTV Staff 'Voyeurs,'" THE MIRROR, December 7, 2005, at 9.
[43] Frank X. Mullen, Jr., "UNR's camera network raises fear," RENO GAZETTE-JOURNAL, March 13, 2005 at 1A.
[44] Jim Dwyer, "Police Video Caught a Couple's Intimate Moment on a Manhattan Rooftop," N.Y. TIMES, December 22, 2005 at B10.
[45] See notes 19, 21, *supra*.

protections; foundational principles of limited and balanced government; and due-process provisions that are as basic to our notion of a free and open society as the right to speak one's mind in public.

The most basic animating principle of the Constitution – of the American Revolution itself – is limited government. The right of the individual to be left alone from government intrusion undergirds most of the Bill of Rights. Surveillance on the kind of massive and intrusive scale now underway in this country violates these fundamental principles.

A. Fourth Amendment

In finding, in *Katz v. United States*, that the Fourth Amendment protects "people, not places," the Supreme Court held that "what a person seeks to keep private, *even in an area accessible to the public*, may be constitutionally protected."[46] (Emphasis added.)

No court has found that the Fourth Amendment, which protects from "unreasonable searches and seizures" extends to protection from police surveillance of public places.[47] Though some courts have found that the Fourth Amendment can be implicated in the search of private places viewed from a public vantage point.[48]And while the Supreme Court in *Delaware v. Prouse* recognized that "people are not shorn of all Fourth Amendment protection when they step from their homes onto the public sidewalks," and likewise are not "shorn of those interests when they step from the sidewalks into their automobiles,"[49] it has not extended protection to the routine use of video surveillance by state actors. Many courts have found there can be no expectation of privacy in public areas.[50]

Unfortunately, courts have based these holdings on arcane notions of privacy, and have been extremely slow to take account of technological changes. It is important to note that the vast majority of these decisions came before it was possible for state actors to quite literally keep constant watch over us without using human beings at the scene to do so. Some courts have found that certain types of electronic monitoring qualify as a searches or seizures under the ambit of the Fourth Amendment[51], but to date, these holdings have fairly limited scope.

---

[46] 389 U.S. 347, 351 (1967).

[47] The leading case in this area is *United States v. Knotts*, 460 U.S. 276 (1983), which held that "a person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."

[48]. *See United Statesv. Torres,* 751 F.2d 875 (7th Cir. 1984).

[49] *Prouse*, 440 U.S. 648, 663 (1979) (quoting *Terry v. Ohio*, 392 U.S. 1 (1968)).

[50] Again, *Knotts*, *supra* note 10, is the leading case here, but *see also*, *Rodriguez v. United States*, 878 F. Supp. 20,24 (S.D.N.Y. 1995) (holding there is no expectation of privacy on a public street).

[51] *See*, *e.g.*, *U.S. v. Karo*, 468 U.S. 705 (1984) (monitoring of tracking devices which reveal information that could not otherwise be obtained through visual surveillance is a "search" within the meaning of the Fourth Amenmdent); *but cf.* U.S. v. Knotts, 460 U.S. 276 (1983) (monitoring of tracking vices to aid visual surveillance is not a search under the Fourth Amendment)

As I noted earlier, the definition of "public area" has changed significantly with the expanding reach of surveillance technology. There is a growing body of legal scholarship, and some case law, arguing for expanding the definition of "expectation of privacy" to take into consideration the vast leaps in surveillance technology.[52] With a few notable exceptions, the U.S. Supreme Court has been reluctant to recognize that the rapid march of technology can infringe on privacy rights.[53]

B. First Amendment

At the heart of our liberties as Americans – and the top of the list in the Bill of Rights – is the ability to speak our minds freely, to join and support unpopular causes, to assemble to criticize our government. Surveillance cameras – particularly the kind of pervasive and all-encompassing cameras we are seeing sprout up across the country – suppress these rights. It has been well documented that surveillance cameras inhibit individual expression.[54] The knowledge that you are being watched causes you to mind your actions.[55] It squelches expressive or silly behavior – human behavior. Political behavior. While it can increase feelings of security for some, it can also inspire feelings of nervousness, guilt and fear that the authorities will note "abnormal" actions.[56] In short, cameras have the ability to turn the democratic cacophony of the town square, the university commons, the steps of City Hall, into sterile and homogenous dead zones.

Unlike the neighborhood beat cop, or even the anonymous officer on patrol; the camera has no identity, no human traits. It cannot be reasoned with, or spoken to. It can't even provide direct protection to the law-abiding – or enforce the law at all. In this sense, it has all the drawbacks of police presence in the American commons – the nervousness, the oppression, the fear – and few of the benefits. It cannot arrest anyone. It can't protect someone walking home alone at night. It can only watch – an activity that is of little comfort to the law-abiding and of little import to the criminal.

---

[52] *See*, *e.g.*, 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); (observing that the indiscriminate collection, for law enforcement purposes, of ostensibly "public" information – like the license plate numbers of patrons of a popular bar – would cause "justified uneasiness" by a "great many people"); *U.S. v. Knotts*, 460 U.S. 276, 283 (1983) (holding that while a police installed tracking device was not an unreasonable search or seizure, if "twenty-four hour surveillance" became possible, "there will be time enough then to determine whether different constitutional principles may be applicable."); Christopher Slobogin, "Public Privacy: Camera Surveillance of public places and the right to anonymity," 72 MISS. L.J. 213, 215 (2002) ("It is time to constitutionalize strictures on public surveillance. The advent of sophisticated technology that allows the government to watch, zoom in on, track, and record the activities of anyone, anywhere in public, twenty-four hours a day, demands regulation").

[53] *See Knotts*, *supra* note 11, 460 U.S. 276, 283; *Katz*, *supra* note 6, at 351.

[54] *See, e.g.*, Hille Koskela, The Gaze Without Eyes, Video Surveillance and the Changing Nature of Urban Space, Progress in Human Geography, 24, 2 (2000) at 243-265

[55] *Id*. at 258.

[56] See *generally* Hille Koskela, Cam Era – the contemporary urban Panopticon, 1 (3) Surveillance & Society 292; Heidi Mork Lomell, Targeting the Unwanted: Video Surveillance and Categorical Exclusion in Oslo, Norway, 2(2/3) Surveillance & Society 292 (examines whether surveillance cameras exclude "unwanted" categories of people from the public sphere – the poor, the visually unusual, minorities).

Courts have been vigorous in protecting First Amendment freedoms from government action that has even a chilling effect on freedom of association or expression.[57] Video surveillance has the capacity to seriously infringe these rights, but existing Supreme Court case law does not create a clear path for setting limits on surveillance – at least that which is purely visual.[58]

However, if public activity is expressive – if it includes political speech, such as a rally at a town square – the First Amendment should be implicated. The Supreme Court has rejected a similar argument, in *Laird v. Tatum*.[59] The *Tatum* court recognized that a blatant violation of constitutional rights is not required for judicial remedy – that a mere chilling effect can be sufficient. But it held that in order to be actionable, the plaintiff must show concrete evidence of actual injury.[60] That is a high bar.

But *Tatum* does not necessarily foreclose the possibility that video surveillance could be found to be a violation of First Amendment rights. In *Meese v. Keene*, the court recognized that plaintiffs whose creative efforts had been labeled "propaganda" by the government had standing to complain of a First Amendment chilling effect, though it ultimately found that no such violation had occurred.[61]

Another potential way in which video surveillance can infringe on well-recognized First Amendment rights is by piercing the anonymity of political activists. It is well settled in Supreme Court case law that the government cannot, without significant justification, compel pamphleteers or the organizers or petition drives to divulge their identities.[62]

People who express themselves in public – politically or otherwise – know they will be observed. But for myriad reasons, they may choose to remain anonymous, and they have the constitutional right to do so. Camera surveillance can nullify that

---

[57] See, e.g., *Lamont v. Postmaster General*, 381 U.S. 301, 303-4 (1965) (finding unconstitutional a federal law requiring the U.S. Postal Service to keep a list of all recipients of "communist political propaganda," and requiring recipients to specifically state that they wanted to receive such "propaganda"); *Watchtower Bible & Tract Soc'y of N.Y., Inc. v. Village of Stratton*, 536 U.S. 150, 167 (holding that a local Ohio ordinance requiring door-to-door petitioners to register with local authorities violated First Amendment free expression principles); *NAACP v. Alabama*, *supra* note 8, 357 U.S. 449 (holding that a court order requiring the disclosure of membership lists violated First Amendment free association principles).

[58] Christopher Slobogin, in "Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity," 72 Miss. L.J. 213, *supra* note 14, notes that if cameras are equipped with audio recording capacity, so that they can pick up "private" conversations on the street, their use would probably require a warrant under both the Fourth Amendment, and Title III, see 18 U.S.C. § 2510(2)(2002)(protecting oral communications "by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation").

[59] 408 U.S. 1 (1972).

[60] *Id*. at 11. The court held that the aggrieved party "must show that he has sustained or is immediately in danger of sustaining a direct injury as the result of [government] action."

[61] 481 U.S. 465 (1987).

[62] *See*, *e.g.*, *Talley v. California*, 362 U.S. 60 (1960) (invalidating a ban on anonymous handbills); *Buckley v. Am. Constitutional Law Found.*, 525 U.S. 182 (1999) (striking down Colorado law requiring petition solicitors to wear identification badges).

anonymity. Because a state-of-the-art digital camera's images are far better than a government agent's memory or handwritten notes, the government's ability to link faces with names vastly improves. Furthermore, constant surveillance of a person's movements – now possible with panoramic video surveillance of large swaths of city centers – can reveal associations, addresses and locales that divulge that person's identity. Political action is thus chilled; the First Amendment is thus violated.

As surveillance systems become more sophisticated, the ability of government agents to monitor and track our political affiliations, social connections and even shopping habits increases greatly. With this increased ability comes a greater risk that surveillance will squelch dissent, political movements and free assembly.

There is little doubt that video surveillance technology poses a serious risk to First Amendment liberties, and there is little doubt that as technology improves those risks will increase. It is therefore not only sensible, but also constitutionally imperative, that the public has a chance to at least evaluate, comment on and have some ability to reject the encroachment of video surveillance on the American commons.

IV. Recommendations

As I noted at the outset, I urge the committee to consider three modest proposals – one short-term, the other two longer-term and more complex.

First, the easy and short-term solution: DHS should require that grantees and researchers receiving federal grant money for surveillance cameras do a Privacy Impact Assessment as required under the E-Government Act of 2002[63]. This is a sensible, painless way to ensure that, at the very least, privacy rights are taken into account as American towns and cities erect sophisticated surveillance systems in their public spaces.

Second, the process of approving surveillance cameras must be an open and publicly accountable process. Before communities across the country are enmeshed in a surveillance net covering every our every public and private step, those communities must have a voice in the decision. It would be wildly inconsistent with fundamental American notions of openness and democratic self-governance to continue enshrouding the country in an invisible surveillance blanket.

Third, federal law must be updated. The courts eventually may come around to bringing privacy law into line with the reality of advanced technologies, but until then it is crucial that our elected federal representatives update restrictions, requirements and explicit civil-liberties protections in the face of unprecedented leaps in surveillance technology.

A. Privacy Impact Assessment

[63] Public Law 107-347, 44 U.S.C. 36.

Pursuant to the E-Government Act of 2002, DHS is required to conduct a Privacy Impact Assessment (PIA) to ensure that technology used by the Department sustains privacy protections. But DHS does not require this of local governments that receive DHS grants to install permanent surveillance systems.

For all of the reasons noted above, it is essential for the protection of privacy in the public sphere that DHS require local governments to analyze the impact on privacy that video surveillance systems will have.

As DHS itself notes in its PIA guidelines manual, the Department "should have in place robust protections for the privacy of any personal information we collect, store, retrieve and share."[64]The same should apply to DHS-funded efforts to collect and/or store the faces, images and movement patterns of the people who fall under the gaze of permanent surveillance cameras.

The E-Government Act requires that PIA's be publicly available, and that the agency compiling personal data explain in the PIA 1) what information is being collected; 2) why that information is being collected; 3) the intended use of the information; 4) with whom the information will be shared; what notice or opportunities for consent will be provided for those whose information is being collected; and 4) how the information will be secured. [65]

This is basic information, and the PIA has become standard operating procedure in many government agencies. The burden of requiring that grantees or researchers compile this information is light, but the benefits are great. First and foremost, it will require local governments that want to install permanent video surveillance systems to consider, on a very basic level, the repercussions of such systems for the privacy rights of American citizens. Given the enormous repercussions of surveillance systems for such rights, it is not only logical but also imperative that such considerations be taken into account.

Second, the PIA will provide some form of initial screening for proposed surveillance projects – a device with which local governments and DHS can evaluate the necessity and appropriateness of surveillance systems. It will help provide local governments and their communities with a basic, publicly available, accounting of what a proposed surveillance system hopes to accomplish, and what liberties may be compromised. It can be a starting point for the kind of discussion about our values that should preface any major expansion of the state's ability to monitor the behavior of its citizens.

Third, the PIA will encourage local governments to formulate concrete policies for determining how surveillance information is stored, accessed and controlled. Again, these are steps that it appears most local governments are not following. The evident

[64] See Privacy Impact Assessments, p. 8, available at http://www.dhs.gov/interweb/assetlibrary/privacy_pia_guidance_march_v5.pdf
[65] 107 P.L. 347; 116 Stat. 2899.

absence of any kind of security protocols is of great concern. It suggests that many local governments have no standard operating procedures in place to ensure that sensitive information is not abused. The lack of policies and procedures is an open invitation to the kinds of abuses we have already seen take place in New York City, Reno Nevada and elsewhere.

As I noted earlier, everyone can agree that security is a legitimate source of great concern after the attacks of September 11. Likewise, there is broad consensus that new technologies can be of assistance in ensuring that our communities stay safe. Those technologies should be allowed to flourish – but not without any oversight or public accountability. Not without some consideration of the very real risk to our liberties, and even our security, that these technologies pose.

We can, and should, use the best technology available to make us safe. But we also can, and must, ensure that that technology is used appropriately and with due consideration of civil liberties. I urge DHS to require privacy impact assessments in grant applications for video surveillance systems.

B. Federal Dialogue and Federal Regulations

Federal law must be updated to keep pace with the rapid expansion of visual surveillance technology. At the very least, it is crucial that there be a discussion, at the federal level, about the serious privacy concerns implicated by permanent video surveillance. To date, there has been a single Congressional hearing devoted to the topic in the last five years, and another hearing that was tangentially related.[66] It may be that Americans are willing to forego some liberties in the name of security, but that decision must be made with the full benefit of robust public debate; Congress must at least address the question. To date, it has not.

The Electronic Communications Privacy Act of 1986[67] can provide some guidance in how to protect civil liberties in the face of extremely rapid technological growth. In 1986, Congress passed the Act in response to concerns about the erosion of civil liberties brought about by technological changes. While the Act extends only to "aural" communications and is therefore inapplicable to silent video surveillance[68], its strictures can provide something of a model in how to both allow for the growth of technology and protect privacy and other constitutional rights.

However Congress chooses to address the problems, it must address them. The slow pace of the courts, combined with the breakneck speed of technological advances,

---

[66] See note 2, *supra.*

[67] 16 U.S.C. § 2510 et seq.

[68] *See United States v. Falls,* 34 F.3d 674, 679-80 (8th Cir.1994); *Koyomejian,* 970 F.2d at 538-41; *United States v. Biasucci,* 786 F.2d 504, 508-09 (2nd Cir.), *cert. denied,* 479 U.S. 827, 107 S.Ct. 104, 107, 93 L.Ed.2d 54, 56 (1986); *United States v. Torres,* 751 F.2d 875, 880-81 (7th Cir.1984), *cert. denied,* 470 U.S. 1087, 105 S.Ct. 1853, 85 L.Ed.2d 150 (1985).

assures that case law – and in particular Supreme Court case law – cannot keep pace with the erosion of civil liberties brought about by video surveillance.

C. Civil Liberties Impact Assessment

Below is a brief summary of a report released recently by the Constitution that recommends a broad set of policies and procedures for adoption by local governments contemplating installing video surveillance systems.

I have attached a copy of their report to my prepared statement.

The Constitution Project's recommendations are more detailed than my recommendations, but are similarly a common-sense approach to ensuring the kind of balance between our constitutional rights and the need for increased security.

1. Core Principles

The civil liberties impact assessment should be guided by a few basic and common sense principles designed to accommodate both the expansion, when necessary, of government-funded surveillance, and the privacy and due process rights of those being watched.

First, public surveillance systems should only be installed or expanded to further a clearly articulated law enforcement purpose.

Second, permanent public surveillance systems should only be installed to address serious threats to public safety that are of indefinite duration. While each community may reach its own conclusions about which threats are "serious" and "of indefinite duration," the Constitution Project recommends – and I agree – that 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.

Third, communities should consider the constitutional rights and principles that can be affected by video surveillance systems. Among these:

- Privacy and anonymity rights.
- Freedom of speech and association.
- Government accountability and safeguards.
- Equal protection and anti-discrimination rights.

Fourth, communities should seek to limit the scope of surveillance systems, where possible, so as to maintain its effectiveness without unnecessarily compromising constitutional rights and values.

Two important limits should be considered: (1)geographic and (2)technological.

(1)*Geographic*. If a particular part of a public park, for example, is a hotbed of criminal activity, a surveillance system should be, to the extent possible, limited to the geographic boundaries of the high-crime area, or at least the public park. Communities should take care to protect from surveillance residential areas or areas where crime is not an issue. It is always easier to later expand the geographic scope of surveillance than to rein it back in once it covers a certain area.

(2)*Technological*. State-of-the-art technology such as infrared detection, high-powered zoom lenses or night vision should be used only if it is clearly necessary. It is these very advances which make surveillance systems capable of invading "public privacy" because they so significantly enhance normal human senses.

Fifth, communities should ensure that surveillance systems come with technological and administrative safeguards to minimize abuse.

Communities should ensure that clear and publicly available procedures are in place to deter, detect and punish abuses. Rules can also provide that stored data be supervised by a government agency independent of law enforcement.

Technological safeguards could include encryption technology to limit control and access to stored surveillance data.

Sixth, the decision to create a public video surveillance system, as well as major decisions affecting its design, should be made through an open and publicly accountable process.

Public input and oversight are critical to ensuring that public officials can be held accountable for the failure – or success – of a public surveillance system. It is therefore imperative that the decision to even have a surveillance system be made in an open forum, by elected or otherwise publicly accountable officials, with the opportunity for public criticism, feedback and suggestion.

2. Procedures for Public Accountability

In order to ensure that public officials are accountable for the decision to install permanent surveillance systems – and accountable for their continuing use – I urge that DHS require that communities receiving money for surveillance cameras undertake a civil liberties impact assessment (CLIA) before installing cameras in public areas.[69]

[69] I will address only permanent surveillance systems in these comments. For temporary systems, a streamlined approach can be used. For details see the Constitution Project's "Guidelines for Public Video Surveillance," *supra* note 25, released May 24, 2006, *available at* http://www.constitutionproject.org/pdf/Video_surveillance_guidelines.pdf, at p. 24.

The fundamental goal of the CLIA is to verify – publicly, so that officials can be held accountable – that a proposed surveillance system is cost-effective, minimally invasive and capable of achieving its stated purpose.

The review process has several steps, which track the core principles I outlined earlier. These can be repeated as necessary if after debate and analysis it becomes clear that the proposal should be modified. While the process is extensive, in the end it is likely to actually help a community save money by cutting back on unnecessary technology and reducing the chances of costly litigation.

I recommend that the CLIA require the following steps:

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

Will the cameras be used ex ante -- for deterring and preventing terrorism or other large-scale harmful events? Violent crime? Misdemeanors?

Or will the cameras be used ex post – as a way of investigating events after they occur? Will the cameras be used for both purposes?

2. **Production of an initial proposal outlining the geographic scope and capabilities of the system**

The proposal should say where each camera is to be installed; the scope of geographic coverage for each camera; and the proposed technical specifications of the entire system.

3. Analysis of whether the proposed system will effectively achieve its stated purposes.

Proposed systems not likely to accomplish their intended goals should be abandoned or redesigned and resubmitted.

.

4. Analysis of the proposal's cost.

Included in this estimate should be all the financial costs of the proposed system, including equipment, installation, training, maintenance, operation and oversight, as well as any economic benefits such as increased tax revenue from business, or improved real estate value.

5. Analysis of the system's impact on constitutional rights and values.[70]

[70] This process is similar to environmental impact reports required of federal agencies when recommending or planning any proposal that will have a significant impact on the environment. 42 U.S.C. § 4332(c). Similarly the E-Government Act of 2002 requires federal agencies to produce a Privacy Impact Assessment (PIA) before they develop or use technology that collects, maintains or disseminates personally identifiable information. Pub. L. No. 107-347, § 208, 116 Stat. 2899, 2921-2922.

The core of the CLIA process, this analysis should document 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 the privacy, freedom of speech and assembly, and other constitutional rights of the surrounding community. The CLIA should also include any proposed technological or administrative safeguards that could mitigate the system's affect on these rights.

Some questions to be answered as part of this process:

Will surveillance be conducted in places where it could be expected to infringe expectations of privacy or anonymity, such as restaurants, nightclubs, medical clinics or political party offices?

Will cameras be able to see into the windows of business offices or residential units?

To what extent will the cameras be able to capture more detail and reveal more information than a law enforcement officer stationed at the scene?

Are the places to be surveilled used for political expression – demonstrations, picketing, leafleting or other First-Amendment protected activities?

How will abuse be prevented? Are there punitive safeguards in place for government agents who would violate the privacy or free-speech rights of residents?

Is the surveillance likely to have a disproportionate affect on racial or ethnic minorities? On the poor? On otherwise marginalized groups?

It is important that the major components of a permanent public video surveillance system[71] not be secret. Secrecy reduces public accountability and prevents public officials from understanding the implications of their actions. To preserve openness and public involvement, I recommend the following:

- The CLIA process should play out before an elected or otherwise publicly accountable body, in public session, with appropriate public notice.

[71] Again, for temporary systems, some secrecy may be required. It is beyond the scope of these comments to address temporary systems. *See* the Constitution Project's "Guidelines for Public Video Surveillance," *supra* note 25, 27, released May 24, 2006 and available at http://www.constitutionproject.org/pdf/Video_surveillance_guidelines.pdf, at p. 24.

- The CLIA and cost-benefit analysis should result 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 comments, make changes and submit a revised proposal, resulting in a revised report.

V. Conclusion

Thank for the opportunity to address the Committee. I look forward to working with you and others to ensure that technological advances and law enforcement needs remain consistent with and supportive of our liberties, norms, and commitment to democratic ideals.