UNIVERSITY OF CALIFORNIA

BERKELEY • DAVIS • IRVINE • LOS ANGELES • MERCED • RIVERSIDE • SAN DIEGO • SAN FRANCISCO

SANTA BARBARA • SANTA CRUZ

SAMUELSON LAW, TECHNOLOGY & PUBLIC POLICY CLINIC
CENTER FOR CLINICAL EDUCATION
SCHOOL OF LAW (BOALT HALL)
BERKELEY, CALIFORNIA 94720-7200
TELEPHONE (510) 643–4800 • FAX (510) 643–4625
www.samuelsonclinic.org

FACULTY
Deirdre Mulligan, Director
Jason Schultz, Associate Director
Jennifer Lynch, Clinic Fellow
Maryanne McCormick, Senior Attorney
Chris Hoofnagle, Senior Attorney
Aaron Burstein, Research Fellow
Jennifer King, Research Specialist

STUDENT INTERNS
Jeremy Brown
Constance Choi
Hilliary Creely
Robert Esposito
Jesse Geraci
Jade Hoffman
Domenico Ippolito
Alyssa Knutson
Solyn Lee
Kathleen Lu
David Hari O'Connell
Igor Pesenson
Genevieve Rosloff
Karla Ruiz
Edward Takashima
Ryan Wong
Kathy Yu

Samuelson Law, Technology & Public Policy Clinic
UC Berkeley School of Law:

Comments for the Record –
CCTV: Developing Best Practices Workshop

Contents

Executive Summary 1
Purpose of Comments 2
The Clinic 2
Expansion of CCTV 3
CCTV and the Character of Public Spaces 3
Lessons from the Workshop 4
Recommendations 6

Executive Summary

These comments convey three core ideas. The first is that CCTV is one tool among many for addressing crime. Studies have raised questions about the effectiveness of CCTV in various contexts. Sound research into the costs and benefits of CCTV should precede decisions about investment and deployment. Second, CCTV, like other technological innovations, is outpacing the development of legal frameworks to guide its deployment and use. The absence of court decisions addressing this nascent technology should not serve as an excuse not to consider the legal and constitutional questions that the possibility of 24/7 surveillance of all individuals within public places poses. Government

officials have an obligation to consider the effect that CCTV has on the rights, liberties, and expectations of individuals in public places and on the capacity of the places to serve the social, political, and community needs for which they are maintained and preserved. Third, there are a growing array of processes and tools—including privacy impact assessments, the civil liberties impact assessment that the Department of Homeland Security is developing, and guidelines that the Constitution Project and others have developed—that governments and police departments can use to craft policies and procedures to align the use of CCTV systems with community needs and the rights and liberties of individuals in public places. In conjunction with investment and deployment decisions based on research about the effective use of CCTV in various settings and for various purposes, the adoption of polices and procedures can improve the possibility that communities will benefit from CCTV systems and that the rights, liberties, and expectations of the public will be respected.

Purpose of Comments

The Samuelson Law, Technology & Public Policy Clinic at the University of California at Berkeley School of Law has prepared these comments in the hope that they would add to the discussions that occurred at the "CCTV: Developing Privacy Best Practices" workshop that the Department of Homeland Security hosted December 17 and 18, 2007. The Clinic also hopes that the comments might offer guidance to the government officials who must grapple with the many complicated issues related to CCTV while they seek to protect communities from crime and terrorism.

The Clinic

The Samuelson Law, Technology & Public Policy Clinic has studied video surveillance systems across the country and has worked with nonprofit institutions and government entities in developing best practices consistent with the needs of police, communities, and democratic values. The government entities with whom the Clinic has worked have included:

- **Department of Homeland Security**: The Clinic developed a method for assessing the impact of CCTV, and DHS used this method when assessing the impact of cameras that it planned to install along a portion of the Arizona-Mexico border as part of its Secure Border Initiative.

- **San Francisco**: The Clinic is working with San Francisco to measure the effect that cameras in the city have had upon crime and to determine how the city might best use video surveillance technologies in the future.

- **Richmond, California**: The Clinic aided the police department in Richmond – one of the highest-crime cities in the country – in developing policies and procedures for a CCTV system that the city plans to deploy this year.

- **Fresno, California**: The Clinic helped the Fresno city council to develop guidelines that would govern the police use of CCTV cameras. These guidelines protected privacy rights while encouraging police to make optimal use of new crime-fighting technologies.

Expansion of CCTV

Through millions of dollars in grants to cities across the country, the Department of Homeland Security is helping to build a massive nationwide CCTV infrastructure. This infrastructure is changing the nature of our public places and threatening our core constitutional liberties. Yet there has been little serious or methodical consideration given to the civil liberties impact or economic rationale for this emerging federally funded network.

In many instances, cameras do not meet communities' economic needs, social norms, or privacy concerns. And police may use other technologies and methods – like additional officers or improved street lighting – to protect communities. Still, CCTV has a powerful appeal. Federal largesse adds to that appeal and creates skewed incentives that encourage local governments to invest in CCTV before they have fully studied its costs and effectiveness or before they have instituted the administrative measures needed to encourage responsible use of those systems and public accountability of the police officers who use them.

CCTV and the Character of Public Spaces

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.

It is now technologically 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 to 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.

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.

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 re-architecting these public places.

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 discussion, after a conversation about the costs and benefits—including the costs to other freedoms and values—of alternative measures for increasing our security.

This discussion will require us to ask questions about when it makes sense – from financial, democratic, and police perspectives – for DHS and other law enforcement agencies to invest in CCTV systems and about how we can best harmonize security concerns with important democratic values like openness, privacy, and oversight. These questions are best answered through a robust public debate that is grounded in rigorous study and likely bolstered at times through protest in the very public places that CCTV systems are already quietly but radically altering.

Lessons from the Workshop

The "CCTV: Developing Privacy Best Practices" workshop featured researchers, police officers, local leaders, privacy officials, advocates, and academic experts as panelists. Ten related themes emerged from their talks. These themes should serve as lessons to those who work on video surveillance issues.

1. **Surveillance Develops Quickly**: The United Kingdom is the most surveilled country in the world. It is famous for its cameras and both privacy and security advocates have cited its extensive CCTV system as a model for what the United States might one day have. The United Kingdom developed its CCTV system quickly – in about ten years. The system in the United States could develop just as quickly. If it does, we have a limited amount of time in which to discuss the impact and appropriateness of large-scale CCTV.

2. **Rushed Adoption**: Federal funding has encouraged some local governments to adopt CCTV. Anecdotal success stories and press accounts of notable CCTV systems have created a bandwagon effect that has inspired additional local governments to do the same. Because of this rush to adopt, local governments have often failed to: a) conduct cost-benefit analyses of CCTV systems; b) involve the public in the CCTV decision-making process; and c) establish mechanisms that officials and the public can later use for evaluating the impact and effectiveness of CCTV systems.

3. **Need for Public Inquiry:** 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.

4. **Uncertain Effectiveness**: Studies have shown that CCTV has less per-dollar effect on crime than other comparably priced strategies like hiring more police officers. Studies have also shown that CCTV does not to deter terrorism but may be helpful in investigating terrorist acts after the fact. CCTV may be Security Theater – that is, better at creating feelings of safety than in creating actual safety. But police officers who have used CCTV systems vouch for their value. One panelist, Chief Robert Keyes of Clovis, California, shared footage that his department used to solve and prevent crimes.

5. **Limited Judicial Guidance**: 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 CCTV systems to watch all individuals who pass through a public space has not been squarely presented to the courts. The Supreme Court may not address CCTV systems for decades – if it ever does – and by then governments will have sunk hundreds of millions more dollars into the systems.

6. **Misuse Occurs**: Misuse is often difficult to detect. Cameras can zoom or follow without making any noise or leaving any physical trace. For each episode of misuse that becomes public, there are probably countless more that do not. The episodes of misuse – sometimes referred to as "horror stories" – that the press has reported have included: the installation of cameras in a school locker room; police officers using a helicopter and thermal imaging device to record a couple's intimate moments on a high-rise terrace; and an officer emailing footage of a suicide to a friend and setting in motion the events that led to the posting of the footage on a pornographic website.

7. **Inadequate Regulation**: Misuse could result from the conduct of rogue actors. But it is very possible that it also results from inadequate regulation. Most police departments do not have written policies and procedures governing the use of CCTV systems. Those that do often rely upon documents that fail to address such issues as accountability or applicability of public records acts to footage.

8. **Best Practices**: Policies and procedures provide a guide to proper conduct but are not self-enforcing. Police supervisors cannot constantly monitor officers, and oversight boards cannot account for every moment that officers are on duty. To ensure that officers use CCTV systems properly at all times, the law enforcement community must also encourage CCTV best practices. Organizations like the International Association of Chiefs of Police and state standards boards must promote such best practices through instructional literature and training.

9. **Impact on Civil Liberties and Public Places**: The significant role of public places in deliberative democracy and in individuals' daily lives, require us 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. 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.

10. **Improving Technology**: Current CCTV systems are highly advanced. They are integrated networks that increasingly feature intelligent software that can be programmed to detect suspicious behavior and that could one day recognize human faces. Devices like license plate readers, which New York City is installing in Lower Manhattan as part of its Ring of Steel, could soon track our geographic movements and ultimately link into databases related to vehicle insurance and other matters. The closer that CCTV technology moves to this point, the more invasive it becomes and the greater the threat that it poses to privacy rights and democratic values.

Recommendations

The Clinic has developed five recommendations based upon the lessons discussed in the previous sections. These recommendations help to advance key goals like public process and accountability. Officials at all levels of government could benefit from reflecting upon these recommendations, but some of the recommendations will obviously be more appropriate to certain levels than to others. The recommendations are as specific as this brief document will allow but in some instances refer the reader to other sources that cover the relevant topics in more detail.

1. **Public Process**: Local governments should provide the public with opportunities to participate in the process by which decisions are made about whether to install, expand, or otherwise change CCTV systems. These opportunities would allow the public to consider the social and economic costs and benefits of the proposed installation, the established technical limitations, and the policies and procedures that would govern the system and guard against misuse. The CLIAs and PIAs discussed in Recommendations 2 and 3 could form an integral part of this public process.

2. **Civil Liberties Impact Assessments (CLIAs):** CLIAs measure the impact that CCTV systems could have upon constitutional rights and civil liberties. Local governments should conduct them before installing, expanding, or otherwise upgrading CCTV systems. The DHS Office of Civil Rights and Civil liberties is currently developing a CLIA template. Local governments may want to consider using this template as a basis for their own CLIAs. The primary goal of a CLIA is to verify – publicly, so that officials can be held accountable – that a proposed surveillance system is: a) cost-effective; b) minimally invasive; c) capable of achieving its stated purpose; and d) consistent with our shared commitment to protecting the civil rights and liberties of all individuals.

   While conducting a civil liberties impact assessment requires an extensive process, 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. A CLIA would consider such questions as:

- 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 marginalized groups?

3. **Privacy Impact Assessments**: PIAs determine the impact that CCTV systems will have on privacy rights. The e-Government Act of 2002 requires DHS to conduct PIAs and to ensure that the technologies that the agency uses respect certain privacy interests. DHS should require state and local governments that are applying for grants for CCTV to conduct PIAs. Attaching such a requirement as a grant condition would be consistent with the spirit of the e-Government Act. Even if DHS does require local governments to conduct PIAs, however, local governments should choose to conduct them because of the benefits that they offer.

   There are three such benefits. First, PIAs require local governments to consider the repercussions of CCTV systems. Second, they help to provide local governments and their communities with a basic accounting of what a proposed surveillance system hopes to accomplish and what liberties may be compromised. Third, they encourage local governments to formulate concrete policies for determining how surveillance information is stored, accessed, and controlled.

   DHS conducted a PIA for the CCTV system that it planned to install along the Arizona-Mexico border as part of the Secure Border Initiative.[1] This PIA – along with the official PIA agency guide that DHS has issued[2] – could serve as a model for local governments that wish to conduct PIAs of proposed CCTV systems. A PIA should ask questions such as:

   - What system design choices were made to enhance privacy?

[1] Privacy Impact Assessment for the SBInet Program, Department of Homeland Security (2007), available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_sbinet.pdf.
[2] Department of Homeland Security, Privacy Impact Assessments: Official Guidance (2007), available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_guidance_may2007.pdf.

- Is notice provided to potential subjects of video recording that they are within view of a CCTV camera?
- How long is footage stored?
- Who will be able to delete, alter or enhance records either before or after storage?
- How is information transmitted or disclosed to external entities?

4. **Local Regulation:** Today, it is local communities in partnership with local law enforcement agencies that must determine how best to install and operate CCTV systems. Therefore it is incumbent upon local officials to develop policies and procedures that meet the needs of law enforcement while respecting civil liberties, civil rights and democratic, community values. These policies and procedures must address, at an operational level, the ways that officers may and may not use CCTV systems. They must also incorporate mechanisms that encourage best practices and ensure public accountability.

   The Constitution Project has written guidelines that could serve as a template for departments wanting to develop policies and procedures.[3] The International Association of Chiefs of Police (IACP) and the Security Industry Association have also created guidelines, though those were published in 2000 and the IACP plans to revise them in response to the technological and legal changes that have occurred in the last seven years.

   CLIAs and PIAs address many of the same factors that policies and procedures address and can often provide much of the basis for policies and procedures. The factors that policies and procedures should address include: signage, privacy protections, training requirements, camera feed access, footage access and retention, and accountability.

5. **Federal Legislation**: Federal law must be updated to address the use of advanced visual surveillance technology by the government. 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. 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

[3] GUIDELINES FOR PUBLIC VIDEO SURVEILLANCE: A GUIDE TO PROTECTING COMMUNITIES AND PRESERVING CIVIL LIBERTIES, CONSTITUTION PROJECT (2007), available at http://www.constitutionproject.org/pdf/Video_surveillance_guidelines.pdf.

distributed public surveillance infrastructure it is time for Congress to establish a federal framework to govern public visual surveillance systems.

Deirdre K. Mulligan
Clinical Professor and Director

Jennifer King
Technologist and Research Specialist

Jeremy Brown
Clinic Intern

CENTER FOR
DEMOCRACY
&
TECHNOLOGY
Working for Civil Liberties on the Internet

1634 I Street, NW Suite 1100
Washington, DC 20006
202.637.9800
fax 202.637.0968
http://www.cdt.org

January 18, 2008

CDT Comments on *CCTV: Developing Best Practices*
Docket No. DHS-2007-0076
Submitted via privacyworkshop@dhs.gov

As the December 17-18, 2007 workshop on Closed Circuit Television (CCTV) made clear, there are many good CCTV "best practices" that have been developed by organizations such as The Constitution Project, ACLU, the American Bar Association, the governments of Canada and the United Kingdom, and even the U.S. Park Police. CDT supports these efforts but believes an equally important question is, how can the public be *assured* that video surveillance "best practices" are being implemented in localities where federal homeland security funds are spent?

DHS leadership on this issue is critically and urgently needed. CCTV is but one piece of the nation's growing surveillance infrastructure. Video surveillance is no longer simply about cameras. Greater use and interoperability of technologies like RFID, sensor networks, and facial recognition and other biometrics make the implications of CCTV even more serious. Every day, advancements in technology are enabling individuals to be monitored and tracked like never before. We believe the federal government, which is a major funder of these developments, has an obligation to ensure individual rights are protected.

In these comments, we suggest actions DHS can take to help protect privacy and civil liberties in light of the growing use of CCTV by governments, especially state and local governments.

DHS Should Develop a Mechanism to Evaluate the Effectiveness of Proposed CCTV Installations

Video cameras are not an effective security measure in many situations. There was considerable testimony at the workshop about the unjustified and ineffective deployment of CCTV. From both the security and the privacy perspective, effectiveness should be a threshold question for DHS.

Since September 11, 2001, the Department's Homeland Security Grant Program (HSGP) has granted $23 billion to state and local governments. For fiscal year 2007 alone, HSGP awarded

$1.7 billion in grants.[1] It is our understanding that *millions* of dollars of these grants have been used to purchase CCTV systems. However, DHS has no CCTV-specific application, evaluation or oversight processes.

DHS should create thorough application and oversight processes that specifically focus on the unique aspects and implications of video surveillance. And state and local governments should have the flexibility to spend federal money on alternative solutions that would tackle the same problems – for example, combating street crime with upgraded lighting rather than simply video cameras.

Most importantly, DHS should require CCTV grant applicants to conduct **efficacy and privacy/civil liberties analyses (i.e., cost/benefit analyses)** *before* any CCTV program is funded and *after* the cameras are up and running for a period of time to determine if they should continue. This cost/benefit analysis could be an extension of the "investment justification" already required the Homeland Security Grants Program.[2] It is also consistent with OMB Circular A-102, which requires an analysis of "costs and benefits" including "how the project will benefit the public," and an explanation of "the criteria to be used to evaluate the results and success of the project."

A cost/benefit analysis should at minimum include the following:

- A discussion of the (anticipated or realized) **benefits of CCTV.** This includes asking the threshold questions: **Is video surveillance needed? Will it be effective?** First, this involves articulating the *specific* problem to be solved or goal to be reached. It should not be sufficient to state in general terms that the goal is combating "terrorism" or suppressing "street crime." Rather, the unique needs of the community should be highlighted: for example, protecting a *specific* neighborhood or facility or addressing a *specific* threat. Second, this involves asking, will CCTV help solve the specific problem or achieve the specific goal? Municipalities should be mindful of the difference between using video surveillance to prevent or deter crime and using it to conduct investigations after-the-fact and prosecute criminals. They should also consider lessons learned from other U.S. municipalities or foreign countries, academic studies of effectiveness, and other relevant resources. The benefits analysis should also consider any economic benefits such as increased tourism or property value.
- A discussion of the (anticipated or realized) **financial costs of CCTV**. This must include the cost of monitoring facilities, personnel costs, maintenance and other ongoing costs. A Baltimore representative at the workshop stated that the city has already spent $17

[1] http://www.ojp.usdoj.gov/odp/grants_programs.htm - fy2007hsgp.

[2] HSGP applicants must submit "investment justifications" that describe "each Investment's ability to impact/enhance homeland security preparedness, as well as the ability of the applicant to successfully execute and implement the Investment," FY 2007 Homeland Security Grant Program, *Investment Justification Reference Guide*, 3, http://www.ojp.usdoj.gov/odp/docs/fy07_hsgp_resource_ij_reference.pdf, but there seems to be no framework for evaluating the effectiveness of proposed programs.

million on its CCTV program. Municipalities must consider where the funding will come from and if other programs might be spending priorities.

- A cost/benefit analysis – including assessments of efficacy and the impacts on privacy and civil liberties – must take into consideration the **specific aspects of the proposed or actual system** and not simply weigh the costs and benefits of CCTV generally. This means reviewing features, uses and locations of the system. Features might include pan, tilt or zoom; biometric capabilities such as face recognition and iris scanning; and various kinds of sensors such as for body heat, motion and even RFID tags. Other issues include whether monitoring will be automated or conducted by humans; whether only live feeds will be viewed or if video will also be archived (and if so, for how long and who will have access to it?); and whether the CCTV system will have wireless component.
- Finally, as part of the cost/benefit analysis, municipalities should consider what **alternatives** exist that would be *as or more* effective than CCTV at solving the specific problem or reaching the specific goal but with *fewer* financial costs and costs to privacy and civil liberties; or with the *same* financial costs but with fewer costs to privacy and civil liberties. For example, if preventing street crime in a particular neighborhood is the articulated goal, perhaps better more police foot patrols might be more effective, cheaper, and less threatening to individual rights. Or perhaps putting more money into education, job creation, after school programs, urban redevelopment, affordable housing and drug treatment programs might help get at the root causes of the crime. More flexibility in DHS grants might enable more of this kind of creative problem solving.

DHS Should Require Privacy Impact Assessments as Part of the Application Process

As DHS recognizes in its own operations, if the efficacy of a proposed project is otherwise reasonably assured, it is necessary to **weigh the privacy/civil liberties impact of the program, through a** "privacy impact assessment."[3] This is perhaps the most important part of the CCTV application. Video surveillance can change the relationship between government and the people, facilitate abuses of power, and encourage social conformity. And specific speech and privacy rights under the First and Fourth Amendments can be threatened. The privacy impact assessment should address the full range of fair information practices, including questions such as who will have access, will the video data be combined with other information, how long will the data be retained, and under what circumstances will it be made available through national law enforcement networks.

DHS Should Place Mandatory Privacy & Civil Liberties Conditions on CCTV Grantees

Drawing on existing "best practices" for CCTV, DHS should require state and local governments to follow a basic set of privacy and civil liberties principles as a condition of receiving CCTV

[3] *See, e.g.*, The Constitution Project, *Guideline for Public Video Surveillance: A Guide to Protecting Communities and Preserving Civil Liberties*, 22-23 (2007), http://www.constitutionproject.org/pdf/Video_Surveillance_Guidelines_Report_w_Model_Legislation4.pdf.

grants.[4] **This is necessary to ensure that video surveillance systems – paid for with federal taxpayer money – do not threaten fundamental rights.**

As a guiding framework in developing CCTV best practices, CDT recommends using the Fair Information Practice Principles, which the DHS Data Privacy and Integrity Advisory Committee has endorsed.[5] The best practices should anticipate as much as possible the various optional features and uses of video surveillance systems, as discussed above.

Setting basic privacy and civil liberties standards would not be a big leap from what DHS already requires of HSGP grantees. HSGP grantees already must comply with a range of technical, administrative and contracting requirements and must make a series of "assurances" and "certifications" – promises, for example, to comply with non-discrimination and environmental laws, to put safeguards in place to prevent conflicts of interest, and to operate a drug-free workplace.[6]

The concern has been expressed that mandatory conditions on CCTV grantees might violate the prohibition against DHS being "substantially involved" in a grantee's use of the money (31 U.S.C. §6304). This seems to be a complete red herring. On its face, §6304 is not a limitation on the terms of grants and to so read it would conflict with years of government grant-making practices. There seems to be no reason why conditions to ensure that video surveillance systems do not erode privacy and civil liberties cannot be crafted in a way to avoid violating the statute.

Some also fear that mandatory conditions might seem like regulations. However, if DHS concludes that the requirements it wishes to impose on CCTV grantees resemble regulations, the Department should consult with the Office of Management & Budget regarding the need to promulgate CCTV-specific regulations via a notice and comment procedure.[7]

DHS Should Conduct Privacy & Civil Liberties Oversight and Enforcement regarding Federally-Funded CCTV Deployments

DHS should develop a comprehensive oversight and enforcement program to ensure that CCTV grantees in fact comply with the mandatory privacy and civil liberties conditions. This should include self-reporting, periodic audits and site visits by the Department, and a citizen complaint

---

[4] The Constitution Project, the ACLU, the American Bar Association, the governments of Canada and the United Kingdom, the U.S. Park Police, and other organizations and individuals provided suggestions during the workshop as to what the best practices should be.

[5] *Framework for Privacy Analysis of Programs, Technologies, and Applications*, Report No. 2006-01 (March 7, 2006), http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_03-2006_framework.pdf.

[6] FY 2007 Homeland Security Grant Program, *Program Guidance and Application Kit*, 15-16, http://www.ojp.usdoj.gov/odp/docs/fy07_hsgp_guidance.pdf.

[7] OMB Circular A-102, *Grants and Cooperative Agreements With State and Local Governments*, http://www.whitehouse.gov/omb/circulars/a102/a102.html.

process (perhaps supported by a toll-free number and online form that enable anonymous submissions) that involves prompt investigation by the Department and remediation. DHS should consult with State Administrative Agencies to determine how they can help the cities and counties receiving CCTV grants comply with the conditions. DHS should also outline when funds will be revoked or grants not renewed based on failures to meet the privacy and civil liberties standards.

DHS Should Provide CCTV Resources & Tools for Municipalities

Finally, the Department should create a website "clearinghouse" that provides a suite of CCTV tools and resources for municipalities such as:

- DHS CCTV grant information (including mandatory privacy/civil liberties conditions or, alternatively, recommended best practices)
- Existing best practices from nonprofits, academics, etc.
- Information about other jurisdictions' CCTV programs (U.S. and international)
- Studies of effectiveness
- Vendors who offer privacy-protecting technologies
- Model cost/benefit analysis, which includes efficacy and privacy/civil liberties assessments (before and after installation of cameras)
- Model legislation/ordinances
- Model training curriculum
- Model public surveys (before and after installation of cameras)

Should the Department decide against attaching mandatory privacy and civil liberties conditions to CCTV grants, DHS should at the very minimum put together a comprehensive and detailed list of "best practices" to guide municipalities in implementing video surveillance systems while protecting individual rights.

In summary, DHS has a lot of power and flexibility to show meaningful leadership on the issue of CCTV. There are many ways the Department can help ensure that federal taxpayer money is being spent on video surveillance programs that are effective and do not erode fundamental liberties.

###