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.

###