Statement
Expectations of Privacy in Public Spaces
By Lillie Coney
Associate Director
Electronic Privacy Information Center

Department of Homeland Security
Data Privacy and Integrity Advisory Committee
Full Committee Meeting
June 7, 2006

I would like to thank the Data Privacy and Integrity Advisory Committee for inviting the Electronic Privacy Information Center (EPIC) to offer comments at today's meeting. EPIC is a public interest research center in Washington, D.C. It was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values. EPIC takes public positions only on matters of concern to consumers and as an advocate for civil liberty and privacy protection.

I am pleased to participate in this panel's discussion on "Expectations of Privacy in Public Spaces." Privacy is difficult to define in the abstract, but much easier for individuals to describe in their own context. All too often, this definition is limited to only viewing privacy as a state or condition of being free from being observed or disturbed by other people. Alan Westin, in his work *Privacy and Freedom* described privacy as a condition of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.[1]

There are three prescribed states of privacy: solitude, small group intimacy, and anonymity.[2] The subject of our panel discussion, "Privacy in Public Spaces" falls under the heading of anonymity. Anonymity can be found when a person is in a public place or engaged in public acts. Anonymity in public spaces means that an individual or group of individuals can still anticipate, and benefit from the freedom of not being identified or falling under scrutiny. Anonymity may seem counterintuitive—how could someone expect privacy yet be in a public place, such as walking along a sidewalk, sitting in a park, joining a demonstration, or attending an entertainment event? People in public places are aware that they can be seen, and they in turn can see others, but the key to understanding anonymity is the inability of human beings to recall in great detail their own past.[3]

How does anonymity exist? It exists because people are not engineered to remember, but are designed to forget. Research done to assist law enforcement in better understanding the contributions of eyewitnesses in criminal investigations produced by Mark Kebbell's and

[1] Daniel J. Solove, Marc Rotenberg, and Paul M. Schwartz, Information Privacy Law, Second Edition, p. 41 (2006)
[2] *id*
[3] Donald A. Norman, The Psychology of Everyday Things, Sneak Preview of Forthcoming Books, Los Angeles Times Magazine, P. 4A, March 6, 1988

Gramham Wagstaff's titled *Face Value? Evaluating the Accuracy of Eyewitness Information*, states the following:[4]

> To illustrate the nature of memory, think back to your last journey to work. You will find it hard to recall details of every person or vehicle that you saw during your journey. This is because memory is not like a video camera system. A video camera captures all of the events that are viewed in the direction in which it is pointed, records them and can replay them; our memories cannot do this. Moreover, we do not passively take information and replay it; rather memory is an active, creative process that can be inaccurate for a variety of reasons. For material to be remembered it must go through three main stages. It must be encoded in to memory, stored there and finally retrieved from memory. Problems can occur at each of these stages (for a more detailed introduction to the psychology of memory see Cohen, 1990).[5]

Significant events can become part of long-term memory,[6] but short-term memory[7] is a processing plant that functions with little regard for order and accuracy of events, places, people or things.[8] In our modern digital communication age, we are awash in information; we have the potential to take in more data with the assistance of technology than any generation of people to proceed us. Our minds exist in a hurricane of information, which reinforces the anonymity of privacy in public spaces as a real part of societal expectations of protection from unwanted intrusion or attention.

Under the condition of anonymity, individuals found in public spaces can find privacy because they become part of the "situational landscape."[9] Unless the person is of sufficient notoriety, or a celebrity or public figure they can and do experience the privacy provided by anonymity.[10] Therefore, people can and do expect privacy while in very public places as long as they are conducting themselves in a way that is not seen as extraordinary. The definition of extraordinary does vary based on custom, culture, and social norms. For example, it would probably take a significant event, such as what occurred on September 11, 2001, to imprint long-term memories on the mind of the typical New Yorker walking along an uptown sidewalk.

Police, for example, rarely want to rely solely on a single person's account of a crime--although it may make for dramatic courtroom theater.[11] Good crime investigative techniques rely on sound forensic evidence along with eyewitness accounts that are notated based on well-developed rules for questioning witnesses to an event or crime.[12]

---

[4] Mark R. Kebbell, Graham F. Wagstaff, Police Research Series Paper 102, Face Value? Evaluating the Accuracy of Eyewitness Information, Research Development Statistics, March 1999, available at http://www.sosig.ac.uk/roads/cgi-bin/tempbyhand.pl?query=922267767-17783&database=sosigv3

[5] *id.*

[6] Harvard Medical School's Consumer Health Information, Types of Memory, available at http://www.intelihealth.com/IH/ihtIH/WSIH000/31393/31397/347125.html?d=dmtContent

[7] *id*

[8] Norman, *supra* n. 3.

[9] Solove, Rotenberg, Schwartz, *supra* n. 1.

[10] Kebbell and Wagstaff. *supra* n. 4. P. 9

[11] Solove, Rotenberg, Schwartz, *supra* n. 1

[12] *id*

> However, it is known that the quality of eyewitness evidence can vary - and does not necessarily correlate with the confidence of the witness. Indeed, research in the USA has shown that inaccurate eyewitness testimony is the main factor leading to false convictions. This research looked at cases in which it could be demonstrated fairly conclusively (for example, through DNA testing) that individuals had been convicted of crimes they did not commit (Huff, Rattner and Sagarin, 1996).[13]

Anonymity is a key component of privacy, but today it is under pressure by the expanded use of surveillance technology, specifically the expanded use of Closed Circuit Television (CCTV). In the EPIC and Privacy International publication, *Privacy and Human Rights: An International Survey of Privacy Laws and Developments 2004*, it is noted that CCTV systems are increasingly being used to monitor public and private spaces. CCTV has grown significantly from use by companies to protect personal property to becoming a tool used by law enforcement authorities for surveillance of public spaces. Great Britain is a leader internationally in the use of CCTV technology with an estimated 150 to 300 million British Pounds spent each year to increase the video surveillance network.[14]

The effort is impressive to law enforcement officials, and in 2002 it was reported that the Mayor of Washington, D.C., wanted to replicate the British CCTV network for our nation's capital. The District of Columbia city government did one key thing in implementing CCTV they developed guidance on the use of the technology.[15]

After the September 11th attacks, US policymakers and security and intelligence services are increasingly advocating the automation of policing functions within society. They are turning toward video surveillance technology as the answer to terrorist threats and the public's demand for security. However, important questions need to be addressed before uncritically accepting the routine surveillance of public spaces, including whether video surveillance is an effective tool for post-crime investigation; a remedy for crime prevention and deterrence, and whether it is an appropriate security measure in terms of civil liberties protections.

In testimony provided by EPIC's Executive Director Marc Rotenberg to the District of Columbia City Council there were three critical points made about the broad public adoption of CCTV technology for surveillance purposes.[16]

First, the use of surveillance cameras raises far-reaching Constitutional questions that implicate the rights of citizens, and most significantly people who engage in peaceful public activities while in public spaces.[17]

---

[13] Kebbell, Wagstaff, *supra*, n. 4
[14] EPIC and Privacy International, Privacy and Human Rights: An International Survey of Privacy Laws and Developments, p. 95, (2004)
[15] Metropolitan Police Department, Notice of Proposed Rulemaking on Closed Circuit Television Cameras, see http://www.dcwatch.com/police/020613.htm
[16] Marc Rotenberg, Testimony before the District of Columbia City Council, Committee on the Judiciary, Public Works, and the Environment, June 13, 2002. http://www.epic.org/privacy/surveillance/testimony_061302.html
[17] *id*

Second, the benefits of video surveillance systems as a means to reduce crime and deter terrorism have been significantly overstated. Studies from London, England and Sydney, Australia make clear that the value of cameras is overstated and that money is better spent on officers than on cameras. Moreover, the particular effort to promote the use of face recognition technology may be one of the biggest corporate boondoggles in recent history, costing taxpayers hundreds of millions of dollars with little benefit in return.[18]

Third, these systems are being interposed in public settings without the benefit of uniform guidelines that equally balance privacy and security. Some efforts at rulemaking in this regard disregard the important privacy protection of anonymity as if it does not exist. These rules also may take too restrictive a view of the expectation of privacy and First Amendment protected activities. Many of these proposed systems of public surveillance lack adequate means of independent oversight. The reporting requirements are vague, the policy on usage and retention may be insufficient, the definitions are too narrow and the auditing is too limited.[19]

I. USE OF SURVEILLANCE CAMERAS IMPLICATES CONSTITUTIONAL RIGHTS

Some have stated that the legal question concerning video cameras in public spaces is simply whether one has a reasonable expectation of privacy in a public place. I believe that this perspective fundamentally misstates the Constitutional interests at stake in this debate.

There is no dispute that the police have a critical role in protecting public safety. This is particularly true when a large number of people are gathered for political protest. Protesters, as well as residents and tourists, have an interest in ensuring that public assemblies are peaceful and do not endanger persons or property. However, there are risks of misuse or abuse of the system. Studies have shown that there is a serious risk of race discrimination: black males are disproportionately scrutinized when such cameras systems are used.[20]

I want to be clear that this concern about surveillance of Constitutionally protected activity is more than theoretical. Shortly after EPIC learned of the plan to install video cameras in public places, we submitted a series of Freedom of Information Act to several agencies in the District. A response that we received from the United States Park Police is particularly revealing.

The documents that we obtained contain individual logs of the aerial surveillance conducted by the District of Columbia Metropolitan Police (MPD). I would like to call your attention to the activities of surveillance by the MPD.

- On October 16, 2000, the United States Park Police of the National Mall of the Million Family March undertook aerial surveillance.
- On January 22, 2002, the Park Police of the pro-life demonstration to the Supreme Court conducted aerial surveillance.

[18] *id*
[19] *id*
[20] NACRO CCTV Study at 4; Clive Norris and Gary Armstrong, The unforgiving Eye: CCTV surveillance in public space, Centre for Criminology and Criminal Justice at Hull University (1997).

- On that same day, the FBI conducted aerial surveillance of the pro-life demonstration.
- On January 20, 2001 the Metropolitan Police Department conducted aerial surveillance of the demonstration activity at 7th and Pennsylvania Avenue during the Presidential inaugural parade.
- On January 18, 2001 aerial surveillance was conducted by the MPD of "demonstration activity." The Park Police "provided downlink photos of coffins/demonstrators."

Although all of these incidents implicate Constitutional matters, the last example may be the most significant because it makes clear that video surveillance is specifically undertaken of individuals engaged in political protest. This clearly implicates constitutionally protected freedoms.

It is also clear that aerial surveillance is increasing. Many of the records we obtained concerned the protests in 2002.

- On April 20, 2002, the Metropolitan Police Department conducted a "downlink video of demonstration activity" at Connecticut and Florida.
- On April 22, 2002, the United States Park Police conducted surveillance of demonstrators.
- On April 22, 2002 the Metropolitan Police Department provided a "downlink of MPD Command Center w/demonstrators."

The 2004 New York City case is an example of federal and state law enforcement officials increasingly using camera surveillance systems to track protesters, which can have a chilling effect on freedoms of speech, assembly, and association.[21]

There will be serious Constitutional questions that arise when images obtained by the police are used in trial against a criminal defendant. Particularly with a technology where it is so easy to manipulate digital images and so difficult to ensure the integrity of a digital file, very clear rules for retention, chain of custody, and use must be established.

II. THE BENEFITS OF CAMERAS HAVE BEEN OVERSTATED

What is the formula for calculating the value of CCTV in protecting public safety? There is little doubt that technologies and certain common sense practices reduce crime. Better lighting in public areas, community policing programs, locking car doors, are examples of techniques that have been proven to reduce the risk of car theft, robbery, and street crimes. In the realm of criminal investigation, fingerprint identification, proper processing of forensic evidence, and skilled investigators continue to play the deciding factors in post crime investigations.

It is worth noting Christopher Slobogin's assessments of why CCTV technology might not be that effective as a crime deterrent or crime interdiction tool in his paper *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*.[22]

[21] See EPIC's Protestor Privacy and Free Expression Rights P. at http://www.epic.org/privacy/protest/

> There are many reasons why cameras might not be effective at reducing crime in the areas on which they are trained. To understand why, consider the three ways cameras can, in theory, be useful: (1) they might help spot incipient crime that can be prevented, or at least solved, through immediate action; (2) they might create a record of crime that can be used in identifying and convicting perpetrators at some later point in time; and (3) they might deter crime. In each of these three areas, obstacles to smooth functioning exist.[23]

Hurdles to CCTV being a sole means of crime detection and intervention is the inability of these surveillance systems to function as people do with the capacity to constantly evaluate their environment. The remote real-time monitoring of CCTV information may not remedy the situation when one takes into account that cameras can be disabled or destroyed, and might not have the range to directly observe the scene of a crime. Further, those who are positioned to review the information provided by CCTV might find it difficult to determine if a crime is being committed.[24] The correct identification of a crime in progress may not result in an officer being dispatched to the area, especially if the calculation was made that fewer officers would be needed with the deployment of CCTV technology. The real possibility of false positives and false negatives should be considered. A false positive is when a crime is believed to be in progress and officers are dispatched only to find that no crime has occurred. A false negative is the assessment that no crime is occurring when in fact one has occurred.

An additional complication for the deployment of CCTV for policing functions is that law enforcement officers may avoid responding to crime situations in areas where they are deployed out of concern that the images recorded might open them to investigation.[25] The investigations and trials that followed the disclosure of videos involving police actions, such as the one of Rodney King[26] and more recently Robert Davis[27] make real their concerns.[28]

For CCTV to work as a possible crime deterrent the public must know that the technology is being used in the location. Notice may also result in criminals migrating to other areas to engage in lawful acts.

However the role of CCTV in post-crime investigation following the London bombings last year cannot be disputed. The role of CCTV to prevent crime is questionable, and should not

---

[22] Christopher Slobogin, Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity, Mississippi Law Journel, Vol. 77, Fall 2002, available at http://www.olemiss.edu/depts/law_school/ruleoflaw/pdf/LJournal02Slobog.pdf
[23] *id.*
[24] *id*
[25] *id*
[26] Wikipedia, Rodney King, available at http://en.wikipedia.org/wiki/Rodney_King
[27] Kikipedia, Robert Davis, available at http://en.wikipedia.org/wiki/Robert_Davis_of_New_Orleans
[28] Associated Press, New Orleans Man Beaten By Police Revisits Scene of Struggle, October 11, 2005, available at http://www.officer.com/article/article.jsp?id=26385&siteSection=5,

be cited as a justification for investing in the technology.[29] Though camera surveillance systems are proliferating, studies have found that they have little effect on crime prevention. Great Britain has an extensive surveillance network: London alone has 200,000 cameras, and more than 4 million cameras have been deployed throughout that country. It is estimated that there is one camera for every 14 people and 300 cameras per day see the average Briton.[30] However, this did not prevent the 2005 London Bombings, but did allow for the identification of criminals afterwards.

The study conducted by Booz Allen of the National Capital Area raised significant questions about the value of CCTV. Their report *Counter-Terrorism Plan for National Park Service, National Capital Region*, obtained by EPIC under the Freedom of Information Act, stated that:

> the most effective countermeasure available to the NPS is the beat officer. No computer or other technological device can replace the human officer whose perceptual system and brain far exceed any other device in coming to a logical analytic and conclusion concerning a potential terrorist situation.[31]

The report goes on to recommend integrated detection, monitoring and surveillance, including CCTV, which would "allow surveillance of multiple memorials and sites simultaneously," but then notes "CCTV will not replace the need for an officer to view and assess the situation." This fact challenges the arguments that CCTV technology will save money. The proposal to invest in CCTV instead of hiring more law enforcement officers, or investing in better training and support of community policing is not supported by the research thus far. Crime has a cost component just as the hiring, training, equipping, and fielding of law enforcement personnel. When considering the adoption of CCTV, communities and policymakers must decide what is the real value in crime deterrence or criminal apprehension. Then, they must evaluate what benefits are achievable, if any, with the adoption of CCTV based on these predetermined values.

It is important to note that the benefits of CCTV technology and particularly face recognition technology that may soon follow have been dramatically overstated. A far-reaching study by Dr. Clive Norris and Gary Armstrong of the Centre for Criminology and Criminal Justice at Hull University, *The Unforgiving Eye: CCTV Surveillance in Public Spaces* found that:

> The gaze of the cameras does not fall equally on all users of the street but on those who are stereotypical predefined as potentially deviant, or through appearance and demeanor are singled out by operators as unrespectable. In this way youth, particularly those already socially and economically marginalized, may be subject to even greater levels of authoritative intervention and official stigmatization, and rather than contributing to

[29] Fran Spielman and Frank Main, City plans camera surveillance web, Chicago Sun-Times, Sept. 10, 2004; see generally Privacy International, Overview: CCTV and Beyond, available at http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-65433.
[30] EPIC, Spotlight on Surveillance, D.C.'s Camera System Should Focus on Emergencies, Not Daily Life, available at http://www.epic.org/privacy/surveillance/spotlight/1205/default.html
[31] Booz Allen, Counter-Terrorism Plan for National Park Service, National Capital Region, Report.

social justice through the reduction of victimization, CCTV will merely become a tool of injustice through the amplification of differential and discriminatory policing.[32]

According to a second study in Sydney, Australia, the CCTV system produced one arrest in 160 days. The study concluded, "Before limited resources are spent on surveillance cameras, close attention must be paid to the claimed benefits."

III A NEED FOR UNIFORM STANDARDS

A GAO Report found that the justification for implementing the new surveillance system was to "among other things, to facilitate crowd management during large demonstrations; officials also indicated that the system could also be used to combat terrorism."[33] Other justifications for the adoption and use of CCTV technology are crime prevention and post crime investigation.

The public concern over the use of video recording technology's use to unknowingly record individuals was so great that the 108th Congress addressed the issue in the Video Voyeurism Prevention Act of 2004, which became public law 108-495.[34] The law amended the federal criminal code to prohibit knowingly videotaping, photographing, filming, recording by any means, or broadcasting an image of a private area of an individual, without that individual's consent, under circumstances in which that individual has a reasonable expectation of privacy. Congress defined "a reasonable expectation of privacy" to mean both private settings and public situations.[35] The law created an exemption for lawful law enforcement, correctional, or intelligence activity, but it did not require that they create guidelines for CCTV surveillance. These guidelines, which should include audits of the information gathered, and routine-reporting requirements would go a long way in allaying concerns about misuse or abuse of recorded images obtained in the course of an investigation.

Last year, four security officers in Merseyside, Great Britain, were charged with voyeurism, accused of using street surveillance cameras to peer into a private home to spy on a woman.[36] A D.C. Council investigation last year found wrongdoing by police during demonstrations in 2002 and that D.C. Police Chief Charles H. Ramsey and other police officials

---

[32] Clive Norris and Gary Armstrong, The Unforgiving Eye: CCTV Surveillance in Public Spaces.
[33] Government Accounting Office, Video Surveillance: Information on Law Enforcement's Use of Closed-Circuit Television to Monitor Selected Federal Property in Washington, DC, GAO-03-748, June 2003
[34] Library of Congress, Thomas, see: http://thomas.loc.gov/cgi-bin/bdquery/z?d108:s.01301:
[35] Senate Bill 1301, Enrolled and Passed by Both the House and the Senate, http://thomas.loc.gov/cgi-bin/query/D?c108:17:./temp/~c108hpa03g::, "`(5) the term `under circumstances in which that individual has a reasonable expectation of privacy' means--

`(A) circumstances in which a reasonable person would believe that he or she could disrobe in privacy, without being concerned that an image of a private area of the individual was being captured; or

`(B) circumstances in which a reasonable person would believe that a private area of the individual would not be visible to the public, regardless of whether that person is in a public or private place."
[36] Emma Gunby, Council Workers Bailed In 'Peeping Tom' Case, Press Association, Aug. 23, 2005.

conspired to cover up evidence of such wrongdoing.[37] The Council's Judiciary Committee submitted a March 2004 report detailing numerous transgressions by D.C. police:

- Metropolitan Police Department use of undercover officers to infiltrate political organizations in the absence of criminal activity and in the absence of policy guidance meant to protect the constitutional rights of those individuals being monitored.
- A pattern and practice of misrepresentation and evasion on the part of leaders of the Metropolitan Police Department with regard to actions by the Department.
- Repeated instances of what appear to be preemptive actions taken against demonstrators including preemptive arrests.
- Failure of the Metropolitan Police Department to effectively police its own members for misconduct associated with demonstrations.
- Failure of the Metropolitan Police Department to acknowledge and to protect the rights of individuals to privacy, and to free speech and assembly.
- Repeated instances of violating the Department's own guidelines for handling demonstrations contained in the Standard Operating Procedures for Mass Demonstrations, Response to Civil Disturbances, and Prisoner Processing including guidelines on use of force in defensive situations, de-escalation in crowd control, and predicates required for mass arrests.

It is also important for policy and decision makers to be mindful of the march of technology. New CCTV systems are capable of recording images, that allow easy archiving, recovery, and sharing of information. Enhanced features include night vision, computer assisted operations, thermal imaging, and motion detection facilities that help improve the operator's attention to the images being relayed. The clarity of the images recorded is of high resolution and many systems can allow the reading of newspaper print at a hundred meters.[38] The advances that will be made in CCTV technology with the perfecting of other applications, such as facial recognition and the scanning of intimate areas between the skin and clothing are also reasons to develop guidance to regulate their use.[39]

The federal government is spending an increasing amount of money on surveillance technology and programs at the expense of other projects.[40] In fiscal year 2006, the federal government planned to add facial recognition checks to all visa applications, which already include fingerprint biometrics.[41] Although the technology has not proven itself in deployment in airports and city streets, the push continues to forge a path to everyday urban and suburban life.

---

[37] District of Columbia Council, Judiciary Committee, Report on Investigation of the Metropolitan Police Department's Policy and Practice in Handling Demonstrations in the District of Columbia at 1 (Mar. 24, 2004), available at http://www.dccouncil.washington.dc.us/patterson/kathypatterson.org/p.s/prinfo/MPDReportFinal5304.doc and http://www.epic.org/privacy/surveillance/spotlight/1205/mpdrep5304.pdf.

[38] Privacy and Human Rights, *supra* n. 12

[39] *id*

[40] EPIC, Spotlight on Surveillance, Facial Recognition Systems Have an Ugly Effect on Personal Privacy, available at http://www.epic.org/privacy/surveillance/spotlight/1105/default.html

[41] *id*

Tampa is one of the U.S. cities that has used facial recognition technology in concert with camera surveillance systems to surreptitiously scan the public.[42] In August 2003, Tampa stopped using the system, supplied by Identix, because of its failures. "It's just proven not to have any benefit to us," said a police department spokesman.[43] The [44]Tampa system is also an example of the privacy risks created by such facial recognition systems. What began as system to catch criminals became a system to find people who might have information for which the police are searching. That is a poor reason to invade the privacy of the general public. With such systems, a person can be scanned without her knowledge or consent. A person's "suspect activity" may be no more than walking around a popular nightlife area.[45]

Despite this poor history, facial recognition systems still are being used. The Defense Department spent $1.6 million to pay Identix for researching facial recognition technology. The Massachusetts Registry of Motor Vehicles recently spent $1.5 million in federal funds for facial recognition systems supplied by Digimarc. Virginia Beach, Va. used $150,000 in federal funds, plus $50,000 of its own funds, for a facial recognition technology-enabled camera surveillance system supplied by Identix. The Texas Department of Public Safety recently contracted with Identix to pay $1.8 million to upgrade its systems to include facial recognition capabilities. Pinellas County, Fla. used $8 million in federal grants to outfit patrol cars, jails and an airport with computerized facial recognition systems supplied by Viisage Technology. The Los Angeles police department is using handheld facial recognition devices supplied Neven Visions. Once again, a person could be merely walking down the street and have a facial recognition device focused on her.

CONCLUSION

Local, state, and federal law enforcement agencies must develop a healthy perspective about transparency in the use of CCTV systems. Transparency is a key component of a functioning healthy democracy. It can be translated into public policy decisions that allow citizens, policymakers, and the media to assure themselves that a local, state or federal government agency is functioning as intended. In this context, the process of providing transparency is referred to as "open government." Open government can be accomplished in a number of ways, which may include: public meetings, public rulemaking notices, reasonable public comment periods, access to rulemaking proceedings, official reports, and open records laws. The application of CCTV technology by law enforcement or for national security should not be excluded from open government objectives. In addition to the methods described, the adoption of CCTV technology may require additional opportunities for public comment that facilitate the participation of those members of the public with relevant skills and training. In this regard, the work of this committee should be a model to local, state, and other federal government agencies.

The City of Baltimore's web site, when conducting a site search for "CCTV" has no documents, while a search for "closed-circuit television" provides one public works document

[42] *id*
[43] *id*
[44]
[45] *id*

with a reference to the technology.[46] However, the District of Columbia's web site search option using a query on "CCTV" retrieved over 8 documents including a policy and procedures manual.

Model guidance should be developed to assist local, state, and federal agencies on the administration of CCTV systems should include strong support of open government procedures that allow public access to the decision making and implementation process. A good start for formulating this guidance to law enforcement and public officials can be found in the American Bar Association's *Technologically Assisted Physical Surveillance Guidance*, which EPIC assisted in developing. There is also the *Guidelines for Public Video Surveillance: A Guide to Protecting Communities and Preserving Civil Liberties* developed by the Constitution Project, which provides eight recommendations on the implementation of CCTV public surveillance systems.

CONTACT

Lillie Coney, Associate Director
Electronic Privacy Information Center
1718 Connecticut Avenue, NW, Suite 200
Washington, DC 20009
1 202- 483-1140 (tel) http://www.epic.org

REFERENCES:

EPIC, Spotlight on Surveillance
http://www.epic.org/privacy/surveillance/spotlight/default.html
EPIC, Video Surveillance Information Page
http://www.epic.org/privacy/surveillance/
The Observing Surveillance Site
http://www.observingsurveillance.org/

Testimony, Marc Rotenberg
Joint Public Oversight Hearing Committee on
The Judiciary Public Works and the Environment
June 13, 2002
http://www.epic.org/privacy/surveillance/testimony_061302.html

Christopher Slobogin
Symposium: Public Privacy: Camera Surveillance of
Public Places and the Right to Anonymity

[46] City of Baltimore, Department of Transportation, Market Place Construction Complete, "The existing Transportation Management Center (TMC) will be completely renovated and state-of-the art closed circuit television surveillance cameras will be installed at major intersections and along gateway arterials, including Interstate 83 within city limits. This new system will improve traffic management by providing a synchronous approach to coordinate the movement of traffic." see: http://www.ci.baltimore.md.us/search?NS-search-p.=document&NS-rel-doc-name=/government/transportation/news.html&NS-query=close+circuit+television&NS-search-type=NS-boolean-query&NS-collection=CityWeb&NS-docs-found=1&NS-doc-number=1

Mississippi Law Journal (Fall, 2002) 77 Miss. L.J. 213

Clive Norris & Gary Armstrong
The Maximum Surveillance Society
The Rise of CCTV
ISBN 1 85973 226 7 (paper)

Guidelines for Public Video Surveillance
A Guide to Protecting Communities and
Preserving Civil Liberties
The Constitution Project
http://www.constitutionproject.org/