METROPOLITAN POLICE DEPARTMENT FOR THE DISTRICT OF COLUMBIA

Expansion of CCTV Pilot Program
Amendments to Chapter 25 of Title 24 of the D.C. Municipal Regulations
Notice of Proposed Rule Making

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

By notice published on June 2, 2006, the Metropolitan Police Department for the District of Columbia requested public comments on its intent to adopt amendments to Chapter 25 of Title 24 of the D.C. Municipal Regulations.[1] The amendments would authorize a pilot program to evaluate the use of closed-circuit television ("CCTV") in preventing, detecting, or investigating crime in D.C. Pursuant to this notice, the Electronic Privacy Information Center ("EPIC") submits these comments to address substantial privacy issues raised by the expansion of the District's CCTV system.

EPIC's interest in Washington, D.C.'s public CCTV system is well documented.[2] In 2002, EPIC launched the Observing Surveillance Project to document the presence of and promote public debate about video cameras placed in Washington, D.C. after the terrorist attacks of September 11, 2001.[3] When the CCTV system was proposed in 2002, EPIC testified before the D.C. Council, and proposed a draft bill to address privacy risks contained in the

[1] Metro. Police Dep't Notice of Proposed Rulemaking, 53 D.C. Reg. 4462 (June 2, 2006), *available at* http://www.grc.dc.gov/grc/site/default.asp?portal_link=lc (click on "DC Laws" in the left column; click on "DC Municipal Regulations and Register"; click on "DMCR and DCR Online"; click on "DCR Online"; click on the "DCR" folder; click on the "2006" folder; click on the "June 2006" folder; click on the "June 2, 2006" folder; then click on "06_02_06_7.pdf").
[2] EPIC, Video Surveillance, http://www.epic.org/privacy/surveillance/.
[3] http://www.observingsurveillance.org/introduction.html.

original proposal.[4] Recently, EPIC testified on this issue before the Department of Homeland Security's Data Privacy and Integrity Advisory Committee.[5]

Introduction

The Metropolitan Police Department's proposal to expand the District's CCTV system from its limited uses to constant, surreptitious surveillance of the public has serious privacy implications. EPIC strongly urges the MPD to reject this expansion. However, if the pilot project goes forward, EPIC urges the MPD to set clear, objective standards for evaluating the success of the expanded CCTV system and create strong regulations, oversight and penalties in order to prevent abuses.

Currently, the MPD has nineteen cameras in the District that are linked through a central observation center located at police headquarters.[6] The cameras are mounted on various buildings primarily in the downtown DC area. They focus on spaces around the National Mall, the U.S. Capitol, the White House, Union Station and other critical installations, as well as major arteries and highways that pass through downtown D.C.[7]

---

[4] *Joint Public Oversight: Hearing before Comm. on the Judiciary on Public Works and the Env't*, City Council of the Dist. of Columbia (June 13, 2002) (statement of Marc Rotenberg, Exec. Director, EPIC), *available at* http://www.epic.org/privacy/surveillance/testimony_061302.html;
District of Columbia Anti-Surveillance and Privacy Protection Act of 2002, EPIC proposed legislation, sec. 4(e), (hereinafter "EPIC Proposed Legislation"), *available at* http://www.epic.org/privacy/surveillance/epic_dcasppa_v1_121202.pdf.

[5] *Expectations of Privacy in Public Spaces*: *Hearing before the Advisory Committee on Data Privacy and Integrity of the Dep't of Homeland Sec.* (June 7, 2006) (Statement by Lillie Coney, Assoc. Director, EPIC), *available at* http://www.epic.org/privacy/surveillance/coneytest060706.pdf.

[6] Metro. Police Dep't Web site *at* http://mpdc.dc.gov/.

[7] *Id*; The current locations of the 19 cameras in D.C. and Virginia are: 1000 block of Jefferson Drive, SW; Pennsylvania Avenue & 15th Street, NW; 14th Street and Constitution Avenue, NW; 700 block of 18th Street, NW; 200 block of Constitution Avenue, NW; 700 block of 19th Street, NW; 19th Street & Dupont Circle, NW; 100 block of Vermont Avenue, NW; 400 block of L'Enfant Plaza, SW; 1100 block of Connecticut Avenue, NW; 1100 block of Pennsylvania Avenue, NW (2 cameras); 800 block of Vermont Avenue, NW; Wisconsin Avenue & M Street, NW; 1000 block of 19th Street, North (Rosslyn, VA); 3600 block of M Street, NW; 500 block of North Capitol Street, NW; 1300 block of Wisconsin Avenue, NW; 300 block of Independence Avenue, SW. *Id*.

The cameras are able to pan at 360 degrees and tilt at 180 degrees.[8] The cameras can also link with selected other public agency video networks, such as traffic cameras operated by the District Department of Transportation.[9] The camera system was developed by Axis Communications, a Swedish firm that has supplied multiple U.S. cities with such surveillance systems.[10] The MPD now proposes to dramatically expand this system of public surveillance.

I. MPD Should Retain Its Strong Public Notification Requirement

In § 2501.10 of the current regulations, the District requires public notice prior to any installation of CCTV.[11] The MPD's proposed regulations would delete § 2501.10, leaving a much weaker public notification requirement. EPIC urges the MPD to keep its strong public notice requirement.[12]

Currently, § 2501.10 states that "additional permanent cameras will only be installed after public notification has been provided and only in locations that will advance the purposes defined in section 2500 of these regulations."[13] In addition to use during exigent circumstances, the current regulations, under § 2500.2, limit CCTV uses to "(1) help manage public resources during major public events and demonstrations; and (2) to coordinate traffic control on an as needed basis."[14]

Section 2502.1 of the proposed regulations requires the Chief of Police to provide public notification prior to the deployment of additional cameras, and §

[8] *Id*.
[9] *Id*.
[10] Jeffrey Selingo, *How It Works: Online, All the Time, an All-Seeing Surveillance System*, N.Y. Times, Apr. 24, 2003.
[11] D.C. MUN. REGS. tit. 24, § 2501.10 (2006).
[12] 53 D.C. Reg. 4463 (June 2, 2006).
[13] D.C. MUN. REGS. tit. 24, § 2501.10.
[14] D.C. MUN. REGS. tit. 24, §§ 2500.2 and 2500.3.

2502.3 grants the public 30 days to submit comments on the proposed deployment.[15] The proposed regulations also provide exceptions to the notice and comment requirements, including under exigent circumstances, pursuant to a court order, or when the Chief of Police determines that notification would "undermine the camera's crime-fighting utility as described in § 2508."[16] It is this last exception that presents problems, because there are no clear standards for "crime-fighting utility." Vague criteria is listed in § 2508.2:

> The Chief of Police shall, at a minimum, consider the following factors prior to using the CCTV system to combat crime:
>
> "(a) The occurrence of a disproportionately high number of calls for service in the proposed CCTV camera location within the preceding 6-month period;
>
> "(b) Any crimes that were committed in the proposed CCTV camera location within the preceding 6-month period; and
>
> "(c) Any other objectively verifiable information from which the Chief of Police may ascertain whether the health, safety, or property of residents who live in the proposed CCTV location are endangered by crime or other illegal activity.[17]

The proposed amendments state that once the cameras no longer "provide any additional crime-fighting utility," the public will be notified and the cameras will be turned off and removed when feasible.[18] However, the lack of clear, strong criteria to determine whether the cameras serve a "crime-fighting utility," when such service would end, or when public notice would undermine such a utility and the fact that these decisions are the sole discretion of the Chief of Police, vests significant power in that one person.[19]

The proposed regulations include a strong definition for public notice or notification: "Notice that includes at a minimum, but is not limited to, publication

[15] 53 D.C. Reg. 4462.
[16] *Id.* at 4463.
[17] *Id.*
[18] 53 D.C. Reg. 4464.
[19] *Id.*

in the *D.C.* Register, posting on the MPD website, written notice to the relevant Councilmember, written notice to the relevant ANC Commissioner, and issuance of a press release."[20] Application of the vague "crime-fighting utility" exception would eviscerate this definition, allowing the possibility of the surreptitious installation of cameras on the slimmest of pretexts.

For the above reasons, clear standards are needed for both the deployment and removal of additional cameras, and for public notification of such. EPIC also recommends that the entire D.C. Council, in consultation with the Chief of Police, should decide when notification would undermine the "crime-fighting utility." The power to install and maintain a system of secret video cameras that could record the activities of the residents of the District should not be vested in one person, particularly one who is not elected.

II. MPD Should Clarify the Purpose of the Expansion of CCTV

Section 2500.2 of the current regulations states two purposes for which the CCTV system is "generally intended to be used."[21] The proposed amendments create a third purpose and refer to a proposed new section for further explanation, but do not clarify the purpose to the extent necessary for effective public comment and evaluation.[22] In fact, the proposed amendments raise several additional problems. EPIC urges the MPD to clearly explain the purposes for the expansion of the CCTV system in a way that allows educated and detailed public comment and enables effective evaluation of the pilot program.

[20] *Id.* at 4465.
[21] D.C. MUN. REGS. tit. 24, § 2500.2.
[22] 53 D.C. Reg. 4462 (§ 2500.2).

Currently, § 2500.2 lists the general intended uses as "(1) to help manage public resources during major public events and demonstrations; and (2) to coordinate traffic control on an as needed basis."[23] The proposed amendment to § 2500.2 would create a third intended use: "to combat crime as authorized by § 2508."[24]

In the proposed § 2508, the MPD sets out a vague purpose for the pilot project of "evaluating the effectiveness of the use of video surveillance in preventing, detecting, deterring, or investigating crime in neighborhoods in the District of Columbia."[25] This statement does not aid in the definition of "combat crime" for purposes of further clarifying § 2500.2. Nor does this statement provide any real guidance for evaluation measures at the end of the pilot project.

The current regulations, in § 2501.2, state that the CCTV technology will not replace current policing techniques.[26] However, further elaboration about how the two techniques will interact would help to provide insight into the purpose of the expansion of the CCTV system from managing major events and traffic in specific instances to constant surveillance of the public for the vague "combat crime" purpose.

For the reasons stated above, EPIC recommends more explicit definitions of "combat crime" and information on the interaction between current policing methods and the CCTV system. Without a clearly stated purpose and standards

[23] D.C. Mun. Regs, tit. 24, § 2500.2.
[24] 53 D.C. Reg. 4462 (§ 2500.2).
[25] *Id.* at 4463 (§ 2508.1).
[26] D.C. MUN. REGS. tit. 24, § 2501.2.

for success (as explained below), it will be impossible to have effective, objective evaluation of usefulness and cost-effectiveness of the pilot project.

III. Clear Standards to Evaluate the Effectiveness of CCTV Are Needed

Although, CCTV systems have shown some success in post-crime investigation, studies have found they provide little benefit in the prevention and detection of crimes. Studies have found that, when there is some reduction in crime rates in areas with CCTV, the crime is actually displaced rather than prevented.[27] Neither the current regulations, nor the proposed amendments delineate any measure for evaluation of the pilot project. EPIC therefore urges the MPD to add specific criteria on which its evaluation of the pilot project will be based. The MPD also should further research the benefits of CCTV systems before expanding the District's system.

Several studies have shown CCTV to be ineffectual at decreasing crime rates. The Scottish Office Central Research Unit found that although there were 3,156 fewer crimes in the 12 months following installation of cameras than the average for the 24 months preceding, "the cameras appeared to have little effect on clear up rates for crimes and offenses."[28] In fact, the report stated, that after adjusting the figures to reflect a general downturn of crimes and offenses, there was "no evidence to suggest that the cameras had reduced crime overall in the city centre."[29] Another study, conducted in Sydney, Australia, revealed that CCTV

[27] One study found that for personal crimes, such as robbery and theft, there was displacement of crimes to areas of the city not covered by CCTV. Rachel Armitage, *Community safety practice briefing: To CCTV or not to CCTV? A review of current research into the effectiveness of CCTV systems in reducing crime*, NACRO (May 2002) (on file with EPIC).
[28] Crime and Criminal Justice Research Findings No. 30, The Scottish Office Central Research Unit, July 7, 1999, *available at* http://www.scotcrim.u-net.com/researchc2.htm.
[29] *Id*.

only produced one arrest in 160 days. The study concluded "[b]efore limited resources are spent on surveillance cameras, close attention must be paid to the claimed benefits."[30]

The benefits of CCTV systems have been overstated. Studies have shown that it is more effective to place more officers on the streets than have them watching the CCTV monitors.[31] A study conducted by Booz Allen of the National Capital Area stated, "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."[32] The minimal effects of CCTV on crime rates show that security funds should be spent on more proven methods of preventing and combating crime, such as hiring more police officers.

There are also more simple crime-fighting solutions than the expansion of CCTV, such as installing additional safety features and educating the community on basic safety. In fact, street lighting has been found to be a more effective crime deterrent than constant surveillance under CCTV.[33] Educating the community about self-protection and simple measures that can be taken to reduce crime rates

---

[30] *Id*.
[31] BRANDON C. WELSH & DAVID P. FARRINGTON, HOME OFFICE RESEARCH, DEV. AND STATISTICS DIRECTORATE, CRIME PREVENTION EFFECTS OF CLOSED CIRCUIT TELEVISION: A SYSTEMATIC REVIEW, RESEARCH STUDY 252 (Aug. 2002) (hereinafter CCTV Study), *available at* http://www.homeoffice.gov.uk/rds/pdfs2/hors252.pdf; NAT'L ASS'N FOR THE CRIMINAL REHAB. OF OFFENDERS, TO CCTV OR NOT TO CCTV? (hereinafter NACRO CCTV study), *available at* http://www.nacro.org.uk/templates/publication/briefingItem.cfm/2002062800-csps.htm.
[32] Booz Allen of the National Capital Area, *Counter-Terrorism Plan for National Park Service, National Capital Region* (on file with EPIC).
[33] EPIC & PRIVACY INTERNATIONAL, PRIVACY AND HUMAN RIGHTS: AN INTERNATIONAL SURVEY OF PRIVACY LAWS AND DEVELOPMENTS 100 (2004).

can also be an effective tool to prevent crime. For example, locking car doors reduces the number of auto thefts.[34] Although this seems to be common sense, reminding the public of actions they can take to prevent crimes, is an effective prevention tool.

For the reasons stated above, EPIC urges the MPD to amend the regulations to include specific criteria for measuring the success of the CCTV pilot project. Additionally, EPIC recommends that MPD conduct further research on the benefits and costs of CCTV. EPIC also recommends that MPD explore the option of using CCTV funds for techniques proven to be more effective, such as more officers, additional safety features, and community education efforts.

IV. MPD Should Reassess the Approach to Privacy in the CCTV Policies

The current regulations attempt to respect a right to privacy, but fall short because the MPD fails to recognize an expectation of privacy in public places. Section 2501.5 states that the CCTV system "shall be used to observe locations that are in public view when there is no reasonable expectation of privacy."[35] However, as EPIC has previously testified, there is a right to privacy, specifically anonymity, even in public places.[36] In public places, anonymity is the protection of being identified or anticipating the freedom of not being identified or falling under scrutiny.[37] Therefore EPIC urges MPD not to expand the CCTV system to allow continuous, general surveillance of the public.

[34] Marc Rotenberg, *supra*.
[35] D.C. MUN. REGS. tit. 24, § 2501.5.
[36] Lillie Coney, *supra*.
[37] *Id*.

Moreover, the federal Video Voyeurism Act makes clear that people have an expectation of privacy in public places, and technology that makes possible observation and recording does not eviscerate this right.[38] The Video Voyeurism Act prohibits 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.[39] Although this Act focused on voyeuristic photographs of an individual's "private area," the law reinforces the concept of privacy even in a public space.[40]

Although it seems counterintuitive to expect privacy when walking on a sidewalk or sitting in a park, the inability of the human mind to recall specific information leads to an expectation of privacy. Research conducted to assist law enforcement to better understand the value of eyewitnesses has shown that memory is very different from cameras.[41] Memory cannot capture all the details of a scene and replay them. Memory is not passive; there is a creative process to encoding memories that can create inaccuracies.[42] Therefore, as long as people are conducting themselves in ways that are not seen as extraordinary, they can and do expect privacy.[43] Cameras change this, recording every detail of an

[38] 18 U.S.C.S. § 1801 (2006).
[39] *Id*.
[40] *Id*. "Private area" is defined as "an individual's naked or undergarment clad genitals, pubic area, buttocks, or female breast." *Id*.
[41] Mark R. Kebbell & Graham F. Wagstaff, *Face Value? Evaluating the Accuracy of Eyewitness Information, Research Dev. Statistics*, Police Research Series Paper 102 (Mar. 1999), *available at* http://www.homeoffice.gov.uk/rds/prgpdfs/fprs102.pdf.
[42] *Id*.
[43] Lillie Coney, *supra*.

individual's interaction with the environment passively, without discretion, and making those details available for infinite replay and scrutiny.

As EPIC Executive Director Marc Rotenberg has testified, approaching privacy from the view that the expectation of privacy is diminished when there are others present in one's physical vicinity confuses the subjective expectation of privacy of the observed with the technological prowess of the observer.[44] "[T]he diminished expectation of privacy associated with the presence of others in one's physical vicinity cannot become the standard for hi-powered CCTV system that covertly observes, monitors and records activities for observation by others that cannot be seen and are not known to the subject," he testified.[45] It is contrary to the legal analysis and it will set the District on a downward spiral that will transform our wonderful public spaces into broad-based zones of surveillance.[46] Pursuant to these privacy concerns, EPIC urges the MPD to reject the use of CCTV for general surveillance purposes and reassess its approach to privacy.

V. MPD Should Change the Focus of the Constitutional Protections

Currently § 2504.4 states that operators of CCTV systems "shall not focus on hand bills, fliers, etc., being distributed or carried pursuant to First Amendment rights."[47] While this section seeks to protect First Amendment rights and prevent abuses like those discussed above, it focuses on the wrong subject. As Executive Director Rotenberg testified, "It is not the handbills or fliers that have First Amendment rights, it is the individuals participating in peaceful public protest

[44] Marc Rotenberg, *supra*.
[45] *Id*.
[46] *Id*.
[47] D.C. MUN. REGS. tit. 24, § 2504.4.

that have these rights." This section, as EPIC previously suggested, should make clear that CCTV would not focus on the faces of these individuals and their identity, without indication of an actual threat to public safety.[48]

Evidence has shown that video surveillance has been used to monitor constitutionally protected activities. For example, documents received by EPIC in response to FOIA requests reveal that the U.S. Park Police had monitored the Million Family March in D.C. and pro-life demonstrations to the U.S. Supreme Court. Other documents revealed that the FBI used aerial video surveillance to monitor the same pro-life demonstrations and the MPD used aerial surveillance to monitor demonstration activity on Inauguration Day in 2001. The MPD also conducted aerial surveillance of demonstration activity for which "downlink photos of coffins/demonstrators" were provided by the U.S. Park Police.[49]

VI. Privacy Rights Training Should be Required for CCTV Operators

The use of CCTV for law enforcement purposes presents the potential for misuse or abuse. Particular issues that have occurred with the use of CCTV are race discrimination and voyeurism. The current regulations attempt to addresses the problem of racial discrimination by prohibiting the use of CCTV to target individuals on a discriminatory basis and requiring all CCTV operators to sign a certification that they understand the CCTV regulations. However, studies have shown that discriminatory use of CCTV systems is a serious risk, and there should be detailed requirements for CCTV operators to undergo privacy rights and anti-discrimination training.

[48] *Id*.; *also* EPIC Proposed Legislation § 4(e).
[49] Marc Rotenberg, *supra*.

Implementation of CCTV will have a disparate impact on minorities, as well as youths and the poor.[50] Black males are disproportionately scrutinized when such camera systems are used, studies have found.[51] Voyeurism has also proven to be problematic when CCTV systems are used. In Great Britain, police officers used the cameras to look into a woman's home and spy on her.[52]

The current regulations seek to minimize the risk of misuse or abuse with the District's system. Currently, § 2501.4 prohibits operators of CCTV system from targeting or observing "individuals solely because of their race, gender, ethnicity, sexual orientation, disability or other classification protected by law."[53] Further, § 2503.1 states that only certified operators shall operate the CCTV system.[54] However, the regulations lack adequate education and enforcement requirements to ensure the success of this policy.

The only criterion for CCTV operator certification specified in the regulations is in § 2503.2, which requires all operators to "sign a certification that they have read and understand the CCTV regulations and acknowledge the potential criminal and/or administrative sanctions for unauthorized use or misuse of the CCTV systems." EPIC recommends requiring more affirmative training. For example, all operators, in addition to reading and signing this statement, should be required to attend a special training seminar that explains the privacy interests of potential subjects of observation; the potential for race, class or age

[50] *Id.* (citing Clive Norris and Gary Armstrong, Centre for Criminology and Criminal Justice, Hull University, *The Unforgiving Eye: CCTV Surveillance in Public Spaces*).
[51] NACRO CCTV study at 6.
[52] Emma Gunby, *Council Workers Bailed in "Peeping Tom" Case*, Press Association (Aug. 23, 2005).
[53] D.C. MUN. REGS. tit. 24, § 2501.4.
[54] *Id.* at § 2503.1.

discrimination; and provides explicit instructions on the prohibited uses of the expanded CCTV system.

The potential criminal and administrative sanctions for misuse or abuse of the CCTV systems are vaguely discussed in § 2503.3.[55] This section of the regulation states:

> anyone who engages in the unauthorized use or misuse of CCTV systems shall be subject to criminal prosecution and/or administrative sanctions, including termination. The administrative sanction will depend on the severity of the infraction and shall be taken in accordance with MPD's Disciplinary Procedures and Policies General Order and/or the adverse and corrective action procedures as provided in the District Personnel Manual.[56]

While these sanctions are appropriate, the regulations should include more specific information on the standards and procedures for determination of the severity of the infraction.

Additionally, these regulations do not address the methods for identification of infractions. There should be a detailed method for the public to file complaints regarding the suspected violation of their rights by CCTV systems operators. This method should include specified response times by the MPD or another entity that will conduct the investigations.

Proper notice of camera placement and deployment would also aid in the detection and prevention of misuses or abuses. As discussed in Part I, the notification requirements of the CCTV system for deployment and activation of new cameras was significantly weakened in the proposed regulations by the deletion of § 2501.10 and the addition of sections 2502.1 and 2508. The changes leave much of the deployment and notification decisions to the sole discretion of

[55] *Id.* at § 2503.3.
[56] *Id*.

the Chief of Police.[57] These weakened, vague notification standards exacerbate the potential problems discussed here. Adequate public notification of camera locations and activation reveals the existence of the cameras to the public and provides the public with the opportunity to raise concerns about the location and coverage of the proposed cameras.

VII. The CCTV System Should Have Strong Legal Safeguards

As discussed in Part VI, the current regulations impose sanctions on the misuse or abuse of the CCTV systems. However, more stringent legal safeguards, including judicial authority and proper public oversight, need to be in place to prevent violations of rights potential with the use of a camera system discussed in Parts V and VI. These potential violations include unlawful surveillance of constitutionally protected activities and misuses and abuses of the camera system.

Currently, § 2503.3 imposes potential criminal and administrative sanctions on CCTV operators who misuse or abuse the CCTV systems.[58] Additionally, § 2507 creates a system for periodic audits. These audits are to be conducted by MPD's Office of Professional Responsibility "at least quarterly, to ensure compliance with these regulations."[59] The regulations state that the audits shall be provided to the Mayor and the Council of the District of Columbia.[60] The sanctions for misuse or abuse serve important deterrent and punishment purposes. However, to be fully effective these must be further specified in the regulations, as discussed above in Part VI.

---

[57] 53 D.C. Reg. 4462 – 64; *also supra* Part I.
[58] D.C. MUN. REGS. tit. 24, § 2503.3.
[59] *Id.* at § 2507.1.
[60] *Id.* at § 2507.2.

As previously requested by EPIC, specific reporting requirements need to be put in place.[61] For example, any knowledge of potential violations should be required to be reported to the head of an agency or the Inspector General of the District. Within 30 days of receiving a report of suspected misuse or abuse, the Inspector General and the head of any D.C. agency should submit a written report to the Mayor and the D.C. Council, including any disciplinary action taken or proposed for violations.

In addition to reporting requirements for employees of the District, there should be an established method of filing complaints for the public. The contact information for making a complaint about suspected misuse or abuse, or some other violation of the CCTV system, should be made available with each public notification of a camera deployment, in addition to public postings in newspapers and signage. Also, as EPIC has previously proposed, the regulations should include a private right of action for any person subject to the misuse or abuse of the CCTV system to seek declaratory and injunctive relief, as well as damages.[62]

Finally, EPIC recommends penalties for any violation of the CCTV system, including the recommended reporting requirements. As previously proposed, these penalties should include disciplinary action, including but not limited to dismissal, and administrative fines up to the amount of $5,000.[63]

Conclusion

An expansion of the District's law enforcement CCTV system would have serious privacy implications, therefore strong regulations, oversight, and penalties

[61] EPIC Proposed Legislation § 9.
[62] *Id.* at § 11.
[63] *Id.* at § 10.

are needed to prevent abuses and protect the public's privacy interests. EPIC urges the MPD not to expand the system from one that is deployed for major events and to observe traffic in limited circumstances to one that places the public under constant surveillance. However, if the MPD persists in expanding the CCTV system, EPIC recommends that the MPD: (1) maintain its strong public notification requirement; (2) clarify the purpose for the expansion of CCTV; (3) set clear, objective standards to evaluate the effectiveness of CCTV; (4) reassess the approach to privacy in the CCTV policy statements; (5) change the focus it places on constitutional protections; (6) require increased training to prevent misuses and abuses; and (7) establish strong legal safeguards, including stringent reporting requirements, methods for public complaint, a private right of action, and penalties for violations.

Respectfully submitted,

_____
Marc Rotenberg,
Executive Director

_____
Lillie Coney,
Associate Director

_____
Melissa Ngo,
Director, Identification and
Surveillance Project

_____
Courtney Barclay,
IPIOP Clerk