March 11, 2008

Chairperson Mary Cheh
Committee on Public Services and Consumer Affairs
D.C. Council
1350 Pennsylvania Avenue, N.W.
Washington, D.C. 20004

Dear Chairperson Cheh:

The Electronic Privacy Information Center (EPIC) is submitting this statement for the record for the D.C. Council's Committee on Public Services and Consumer Affairs public hearing held today. The hearing will include a discussion of Bill 17-438, "Enhanced Security at Gas Stations Amendment Act of 2008." Among other things, the bill would require the owners of gas stations in the District to purchase, install and use 24-hour "video surveillance equipment to monitor all pumps at their stations to deter and help solve crimes on their properties" and require the Metropolitan Police Department to "[d]evelop and implement a training system to ensure officers utilize the video surveillance equipment at retail service stations for the purposes of investigating crimes committed at retail service stations."[1]

EPIC has extensive experience on video surveillance issues. 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.[2] When the camera surveillance system (also known as "closed-circuit television" or "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 original proposal.[3] In 2006, EPIC submitted detailed comments when the Metropolitan Police Department sought to dramatically expand the District's CCTV system.[4] That same year, EPIC testified about issue before the Department of Homeland Security Security's Data Privacy and Integrity Advisory Committee.[5] In December 2007, EPIC presented its

---

[1] Bill 17-438, Enhanced Security at Gas Stations Amendment Act of 2008, at §§ 2, 4., *available at* http://www.dccouncil.washington.dc.us/lims/getleg1.asp?legno=b17-0438.
[2] http://www.observingsurveillance.org/introduction.html
[3] *Joint Public Oversight: Hearing before Comm. on the Judiciary on Public Works and the Env't*, *Council of the Dist. of Columbia* (June 13, 2002) (statement of Marc Rotenberg, Exec. Dir., 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), *available at* http://www.epic.org/privacy/surveillance/epic_dcasppa_v1_121202.pdf.
[4] EPIC, *Comments to the Metropolitan Police Department for the District of Columbia on the Expansion of CCTV Pilot Program* (June 29, 2006), *available at* http://www.epic.org/privacy/surveillance/cctvcom062906.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. Dir., EPIC), *available at* http://www.epic.org/privacy/surveillance/coneytest060706.pdf.

proposed best practices for CCTV use at the Department of Homeland Security's Privacy Office workshop on camera surveillance systems.[6]

Bill 17-438 raises several questions about efficacy, privacy, and cost. Among other things, the bill would require the owners of gas stations in the District to purchase, install and use 24-hour "video surveillance equipment to monitor all pumps at their stations" and require the Metropolitan Police Department to "[d]evelop and implement a training system to ensure officers utilize the video surveillance equipment at retail service stations for the purposes of investigating crimes committed at retail service stations."[7] The bill requires business owners to purchase and install the systems "to deter and help solve crimes on their properties." However, there is no evidence to prove that camera surveillance systems substantially deter crime and some evidence that such surveillance systems help in post-crime investigations.

In the District itself there is no evidence that CCTV significantly deters crime or substantially helps to solve crimes. The MPD began deploying cameras in District neighborhoods in August 2006 in order to "combat crime."[8] As of October 2007, there are 73 cameras in the District, according to the MPD.[9] In response to a Freedom of Information Act request from the ACLU of the National Capital Area, the Metropolitan Police Department said, "As of March 17, 2007, the Metropolitan Police Department has made no arrests resulting from information found through camera surveillance."[10] Just last month, the MPD released its annual report on CCTV in the District, and it did not list any convictions brought about by the cameras.[11] It also does not detail the total number of arrests based on camera surveillance data or information found through camera surveillance, but rather described a handful of arrests and cases that remain open even though there was evidence from the cameras.[12]

Before installing or expanding CCTV systems, there must be concrete evidence consisting of verifiable reports of the risks, dangers, and crime rates that demonstrate there is sufficient reason to override the substantial monetary and social costs involved. It

---

[6] Melissa Ngo, EPIC, Senior Counsel, *Presentation at a Workshop on "CCTV: Privacy Best Practices"* (Dec. 18,2007), *available at* http://www.dhs.gov/xinfoshare/committees/editorial_0699.shtm.
[7] Bill 17-438, Enhanced Security at Gas Stations Amendment Act of 2008, at §§ 2, 4., *supra* note 1.
[8] Metropolitan Police Dep't, *Fact Sheet: Use of Closed Circuit Television (CCTV) to Fight Crime in DC Neighborhoods*, Mar. 2007, *available at* http://mpdc.dc.gov/mpdc/frames.asp?doc=/mpdc/lib/mpdc/info/programs/CCTV_neighborhood_FAQ.pdf.
[9] Press Release, Metropolitan Police Dep't, MPD Deploys Additional CCTV Camera in Northwest DC, Oct. 9, 2007, *available at* http://newsroom.dc.gov/show.aspx/agency/mpdc/section/2/release/11960/year/2007.
[10] Letter from Johnny Barnes, Exec. Dir., ACLU-NCA, and Stephen Block, Legislative Counsel, ACLU-NCA, *available at* Phil Mendelson, Chairperson, Comm. on the Pub. Safety & Judiciary, D.C. Council, Regarding the Budget of the Metropolitan Police Department, Mar. 30, 3007, *available at* http://www.aclu-nca.org/pdf/Mendelson3-30-07.pdf, *quoting* MPD response to ACLU-NCA FOIA request, Letter from Erich Miller, Lieut., Metropolitan Police Dep't , to Fritz Mulhauser, ACLU-NCA, Regarding FOIA: 06-570, Mar. 19, 2007 (on file at EPIC).
[11] Metropolitan Police Dep't, *Closed Circuit Television (CCTV) Annual Report 2007* (Feb. 2008) [hereinafter 2007 CCTV Annual Report], *available at* http://mpdc.dc.gov/mpdc/frames.asp?doc=/mpdc/lib/mpdc/publications/CCTV_annual_report_2007.pdf.
[12] *Id*. at 9-10.

must be possible to measure the success of the system to determine whether the considerable expenditure of public resources on a CCTV system justifies the continuation of the program. In this case, it is especially important, as the law would require small-business owners to spend their own funds to purchase and install the systems.

Studies conducted by government agencies in the U.S. and internationally have found video surveillance has little effect on crime rates.[13] In fact, studies have found it is far more effective to spend limited law enforcement resources on adding more police officers to a community and improving street lighting in high crime areas than spending large amounts of money to install expensive technology.[14] In Great Britain, which has an estimated 4.2 million cameras, a 2005 study by the Home Office of the United Kingdom (comparable to the U.S. Department of Homeland Security) determined that CCTV did not reduce crime in 13 of the 14 areas studied.[15]

There are times when CCTV does not help with post-crime investigation, either. The Council does not need to look outside the District area to find an example. In 2005, police in Washington, D.C. concluded a two-year serial arson probe. Thousands of hours of surveillance tapes were examined, including footage from cameras planted specifically by investigators. The arsonist was never caught on tape, but rather, the man who set fire to 45 houses and apartments over the course of three years was identified through DNA evidence found at four of the crime scenes.[16]

Beyond determining the ability of camera surveillance systems to meet the Council's goal, "to deter and help solve crimes on their properties," EPIC also urges the Council to examine the privacy and civil liberties consequences of Bill 17-438. EPIC has previously explained, in testimony and written submissions, that there is a right to

---

[13] *See generally* EPIC AND PRIVACY INT'L, PRIVACY AND HUMAN RIGHTS 85-98 (EPIC 2006);
[13] Brandon C. Welsh & David P. Farrington, Home Office Research, Dev. & Statistics Directorate, *Crime prevention effects of closed circuit television: a systematic review*, *Research Study 252* (Aug. 2002) [hereinafter "Home Office Study on CCTV"], *available at* http://www.homeoffice.gov.uk/rds/pdfs2/hors252.pdf; NACRO, *To CCTV or not to CCTV? A review of current research into the effectiveness of CCTV systems in reducing crime* (June 28, 2002) [hereinafter "NACRO CCTV Study"], *available at* http://www.nacro.org.uk/templates/publications/briefingItem.cfm/2002062800-csps.htm *and* http://www.epic.org/privacy/surveillance/spotlight/0505/nacro02.pdf. In 2002, the British Home Office examined 22 camera surveillance systems in North America and the United Kingdom, and found that such systems had a small effect on crime prevention. *See* Home Office Study at 45.
[14] For more information about camera surveillance and security, *see* Melissa Ngo, "You Are Being Watched But Not Protected: The Myth of Security Under Camera Surveillance" in INTERSECTION: SIDEWALKS AND PUBLIC SPACE (Chain, forthcoming Mar. 2008).
[15] Centre for Criminological Research, *Testimony of Clive Norris, Professor of Sociology and Deputy Director of the Centre for Criminological Research, Sheffield University, at a Hearing of the U.S. Department of Homeland Security's Data Privacy and Integrity Advisory Committee, "Closed Circuit Television: a Review of its Development and its Implications for Privacy"* (San Francisco, CA: June 7, 2006); U.K. Home Office, *The Impact of CCTV: Fourteen Case Studies,* Martin Gill et al., (London: 2005). http://www.homeoffice.gov.uk/
[16] Ruben Castaneda & Del Quentin Wilber, *Arsonist Apologizes But Does Not Explain*, WASHINGTON POST, Sept. 13, 2005; Michael E. Ruane, *Security Camera New Star Witness*, WASHINGTON POST, Oct. 8, 2005.

privacy, specifically anonymity, even in public places.[17] In public places, anonymity is the protection of being identified or anticipating the freedom of not being identified or falling under scrutiny.

Moreover, the federal Video Voyeurism Prevention 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.[18] The Video Voyeurism Prevention 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.[19] 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.[20]

The Council should also determine what would be the cost of this program to the business owners and to the D.C. taxpayers. The District has already spent millions on surveillance cameras. In its annual report on CCTV released last month, the MPD said, "To date, the District of Columbia has invested approximately $3.8 million ($2.3 million for Phase I and $1.5 million for Phase II) to purchase, install and operate the CCTV system. The 18 original homeland security cameras (purchased in 2000) will be replaced in 2008 at a cost of $630,000 in U.S. Department of Homeland Security grant funds" and ongoing maintenance of the system has the "estimated annual cost in fiscal year 2008 of $600,000."[21]

Bill 17-438 would impose considerable cost onto small-business owners, and the public deserves to know the full details of this cost. What would be the price of the cameras? What would be the cost of detailing police officers to use these systems? What would the cost of maintenance of these systems? The public has a right to know if the vendors have been chosen, who they are, what systems they would install, and how much this would cost. It is especially important for the Council and the public to know the reputation of the companies involved.

EPIC has detailed specific privacy conditions that must be in place in order for privacy and civil liberties to be adequately protected.[22] They are:

1. **CCTV Alternatives Preferred:** Video surveillance should be viewed as an exceptional step, only to be taken in the absence of a less privacy-invasive alternative.

---

[17] *See* EPIC testimony and writings, *supra* notes 3-6.
[18] 18 U.S.C.S. § 1801 (2006).
[19] *Id*.
[20] *Id*. "Private area" is defined as "an individual's naked or undergarment clad genitals, pubic area, buttocks, or female breast." *Id*.
[21] 2007 CCTV Annual Report at 10, *supra* note 11.
[22] EPIC, *Privacy Conditions for Video Surveillance*, (Jan. 15, 2008), *available at* http://www.epic.org/privacy/surveillance/epic_cctv_011508.pdf.

2. **Demonstrated Need:** CCTV systems should only be deployed to address a clearly articulated problem that is real, pressing and substantial.

3. **Public Consultation:** The public, the local community, and privacy and security experts should be consulted prior to any decision to introduce video surveillance or implement any significant change to an existing system.

4. **Fair Information Practices:** The use of video surveillance should be governed by an explicit policy based on Fair Information Practices, 1980 OECD Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data, and the Privacy Act of 1974. In any collection, use, disclosure, retention and destruction of personal information, there must be:

    a. **Openness, or transparency:** CCTV operators must make public their policies and practices involving the use and maintenance of CCTV systems, and there should be no secret databases. Individuals have a right to know when they are being watched.
    b. **Purpose specification:** CCTV operators must give notice of the purposes for which the CCTV systems are being created and used. After detailing the purpose of the CCTV system, set clear, objective standards to evaluate the effectiveness of the system. Ensure there is a process to uninstall the CCTV system if it is found to be ineffective at solving or even helping to worsen the problem it was created to solve.
    c. **Collection limitation:** The collection of information should be limited to that which is necessary for the specific purpose articulated. A policy should be established so as to minimize or limit the collection or distribution of personally identifiable information.
    d. **Accountability:** CCTV operators are responsible for implementation of this technology and the associated data collected. CCTV operators should be legally responsible for complying with these principles. An independent oversight office should be created in each jurisdiction where a CCTV system is to be used, and this office should audit and evaluate the system at least annually.
    e. **Individual participation:** Individuals should be able to learn about the data collected about them and rectify any errors or problems in the data. There must be a private right of action so that individuals may be able to police their privacy rights in case of misuse or abuse of the systems.
    f. **Security safeguards:** There must be security and integrity in transmission, databases, and system access. Also, there should be continuing privacy and civil liberties training for CCTV operators. All security safeguards should be verified by independent parties, and the assessments should be publicly disclosed.

5. **Privacy Impact Assessment:** Before implementing any CCTV system, conduct a Privacy and Civil Liberties Impact Assessment to detail how such a system could affect Constitutional rights and civil liberties.

6. **Enhanced Safeguards for Enhanced Surveillance:** Any additional analysis capability added by "smart" cameras or other technology will require corresponding privacy and security safeguards.

In the process surrounding Bill 17-438, the D.C. Council has not met fully these conditions. We urge the Council to implement these conditions before moving forward. We believe the Council, after reviewing Bill 17-438 within the framework of these conditions, will find that traditional methods of policing are far less expensive and far more effective at creating safe communities than video surveillance systems.

Respectfully submitted,

_____

Melissa Ngo
Senior Counsel

ELECTRONIC PRIVACY
INFORMATION CENTER
1718 Connecticut Avenue, N.W.
Suite 200
Washington, DC 20009
(202) 483-1140