Prepared Testimony of
Melissa Ngo
Privacy and Information Policy Consultant and Publisher of PrivacyLives.com
Before the
Committee on Public Safety and the Judiciary of the D.C. Council
At a Hearing on "Video Interoperability for Public Safety" Program

June 2, 2008

My name is Melissa Ngo, and I am a Privacy and Information Policy Consultant and Publisher of PrivacyLives.com. Thank you for inviting me to participate in today's hearing concerning the proposed "Video Interoperability for Public Safety" ("VIPS") Program.

I have worked on privacy and civil liberties issues for several years and recently published a chapter in a book specifically on camera surveillance systems called, "You Are Being Watched But Not Protected: The Myth of Security Under Camera Surveillance." At PrivacyLives.com, I chronicle and analyze attacks on privacy and civil liberties and various defenses against these assaults to show that privacy lives on.

In March, I submitted a statement to the Council concerning the privacy and civil liberty issues surrounding Bill 17-438, which seeks to require the owners of gas stations in the District to purchase, install and use 24-hour video surveillance equipment.[1] I am here today to ask the Council to require that important questions be answered concerning oversight of the Video Interoperability for Public Safety Program, its goals, and its costs (both financially and to privacy and civil rights).

I. Secrecy Surrounds the "Video Interoperability for Public Safety" Program

There is little known about the VIPS program, except for scattered news reports and some public statements from Mayor Fenty and other D.C. government officials. On April 8, in a press release, Mayor Fenty announced the creation of the Video Interoperability for Public Safety Program, which would "connect the city's more than 5200 cameras into one network" and "result[] in a CCTV system that operates 24 hours a day, 365 days a year ..."[2] Mayor Fenty stated that VIPS would not focus solely on crime, instead "the VIPS program will also have an all-hazards approach" and be consolidated under the District's Homeland Security and Emergency Management Agency ("HSEMA").[3] It is unclear what "all-hazards" encompasses. In the same press release, Darrell Darnell, Director of HSEMA, said:

> In developing the VIPS program we were careful to ensure that our use of CCTV monitoring be proportional, legal, accountable and necessary and

that we have safeguards in place that prohibit the release of images except for purposes of crime prevention and detection.

Our guidelines will ensure that cameras are installed at locations based on public safety needs, that the system is used only for the purpose of enhanced situational awareness and not for other labor or employee performance reasons and that we have safeguards in place to prevent improper access to images and maintain records that show access and chain of custody for images.[4]

In news reports and public announcements since then, there has been little elaboration about the specifics of this program. Mayor Fenty and Director Darnell did not discuss VIPS with either the D.C. Council or the District public before announcing the program as a done deal. Yet there are numerous questions that must be answered before the District can even consider creating this massive centralized system of surveillance cameras.

II. Unanswered Questions Regarding Privacy and Civil Liberties

There are numerous unanswered questions concerning how the privacy and civil liberties of District residents and visitors will be protected. On April 8, Director Darnell said there were "safeguards" and "guidelines" for the VIPS program that would protect D.C. residents, yet four days earlier, he told Councilmember Phil Mendelson that the District government had not created regulations for this massive new centralized system.

In a letter to Councilmember Mendelson concerning the Fiscal Year 2009 budget of the D.C. Homeland Security and Emergency Management Agency, Director Darnell said, "Phase one of the [VIPS] program will consolidate CCTV monitoring functions under one roof for four current video user agencies, including DDOT, PSD, DCPS and DCHA. During this phase, HSEMA *will develop* standards for CCTV technology and establish a multi-agency procurement process" (emphasis mine).[5] Also, on April 10, the *Washington Post* reported Director Darnell stating, "we really need to come up with a District-wide policy, to make sure we don't violate any civil liberties and don't co-mingle monitoring functions with police surveillance."[6]

Several Councilmembers have stated that it is extremely problematic to create a massive, 5,200-camera, centralized surveillance system controlled by the District's Homeland Security agency without having privacy and civil liberty safeguards in place. I agree. Government needs to operate transparently in order to gain the trust of the public. To create such a massive surveillance system in secret and then to put so little importance on protecting the privacy and civil rights of the District's residents is to ask for the public to mistrust the D.C.

government. It is also a recipe for misuse and abuse of the system through ignorance or intentional misconduct.

The regulations set out for the VIPS program should follow the universally accepted Fair Information Practices.[7] First, the HSEMA needs to articulate a specific purpose for the VIPS program and how this purpose will be fulfilled by the centralized surveillance system. What measurements will be used to decide if the purpose is fulfilled? Second, there should be transparency in the policies and practices of the VIPS program and HSEMA. Third, the data collection should be limited to the data necessary for the specific purpose that has been articulated.

Fourth, there must be accountability. CCTV operators and other VIPS program employees must be trained on the regulations set up to protect District residents and visitors. These employees must be legally responsible for complying with these regulations. A separate oversight office should be created and required to audit and evaluate the system at least annually.

Fifth, there must be individual participation. Individuals should be able to learn about the data collected on them and rectify any problems in the data. Individuals should have a private right of action so that they may be able to police their rights in case of misuse or abuse of the VIPS program. And finally, there must be strong security protections. There must be security and integrity in transmission, databases, and system access. All security protections should be audited and verified by an independent party and the results of these audits should be made public.

III. Lack of Strong Regulations for VIPS Creates High Risk of Misuse or Abuse of the System

There are myriad reasons for the District to create regulations for the Video Interoperability for Public Safety Program before deploying such a massive surveillance system. But we should focus closely upon the problems that would arise from misuse or abuse of the surveillance system and the data gathered.

Everyone has heard of the police officer who used surveillance cameras to zoom in on women's breasts and buttocks at the San Francisco airport and the New York police officers who used high-powered surveillance cameras to spy on a couple's romantic activity.[8] And people can understand the horror that a person would feel upon learning that a visit to the fertility clinic or addiction-recovery center had been recorded. But there are also specific examples of misuse and abuse of cameras set in schools and in public housing complexes.

Last year, in Tacoma, Wash., a high school official showed parents video of their daughter kissing another girl.[9] The surveillance cameras had been put in place to catch crimes such as vandalism or schoolyard fights, yet the footage was used for a completely different purpose.

More disturbing is what occurred in 2004. A young man's suicide was filmed by a surveillance system in a New York public housing project.[10] The video from the police surveillance camera ended up on Consumption Junction, a Web site describing itself as a purveyor of "free video clips that include shocking moments, brutal stupidity, and a healthy dose of hard core sex."[11] The suicide video was labeled, "Introducing: The Self-Cleansing Housing Project."[12] The young man's foster mother learned the video was on the Web site and she said, "I started healing, and this kicked me backwards. My whole body was shaking."[13]

These examples show clearly that strong regulations need to be in place before VIPS is deployed. These regulations must follow the Fair Information Practices, as I detailed above. District residents must know that someone will be watching these watchers and protecting the rights of innocent individuals.

IV. There Is No Evidence to Show That Camera Surveillance Systems Significantly Cut Crime

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 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 Video Interoperability for Public Safety Program would centralize thousands of public school, public housing, and other cameras under the District's Homeland Security agency, affecting every District resident and visitor.

What is the goal of this massive system? How will the District measure if system achieves this goal? How is it necessary for the District's Homeland Security agency to monitor more than 3,400 public school cameras and 720 public housing cameras?

Studies conducted by government agencies in the U.S. and internationally have found video surveillance has little effect on crime rates. 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]

Though there is evidence that CCTV assists with post-crime investigation, there are also times when CCTV is not helpful to investigators. 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]

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."[17] As of October 2007, there are 73 cameras in the District, according to the MPD.[18] 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."[19] In February, the MPD released its annual report on CCTV in the District, and it did not list any convictions brought about by the cameras.[20] 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.[21]

The MPD's annual report states that violent crime in areas within 250 feet of cameras has dropped by 19 percent since last year, but also finds that there has been a 1 percent increase in violent crime in the rest of the District.[22] The MPD does not conduct any analysis as to whether the crime was simply displaced from the camera areas to other parts of the District, which Councilmember Mary Cheh noted at a March hearing on a bill that would require District gas station owners to purchase and install CCTV systems.[23] At that hearing, Councilmember Cheh requested that the MPD representative conduct such analysis. Councilmember Mendelson and others have raised questions about displacement problems. If any analysis of possible displacement effects in D.C.'s CCTV system has been conducted, the MPD has not yet released this analysis to the public.

There is also the question of cost. Director Darnell has said that the District will be using federal Homeland Security grant funding as well as the District's own funds to create and maintain this massive surveillance system. This raises yet more questions. What other homeland security programs are not being funded because the money is diverted to the Video Interoperability for Public Safety Program? Are officers being reassigned from street patrol or other

duties in order to watch over this centralized surveillance program? Is this plan more effective and cost-effective than other crime-reduction techniques, such as adding more officers to patrol neighborhoods and school zones?

V. Conclusion

Before the Video Interoperability for Public Safety Program is deployed, the District government must answer the questions that have been raised here today. District residents deserve to know if this program would in fact improve their safety or if it is yet another attempt to slap a Band-Aid on a gushing wound and call the problem solved.

Melissa Ngo
Privacy and Information Policy Consultant
Publisher of PrivacyLives.com
E-mail: privacy [at] privacylives.com

June 2, 2008

End Notes

[1] Melissa Ngo, EPIC Senior Counsel and Director of the Identification & Surveillance Project, Statement to the DC Council Opposing Expanded Camera Surveillance Under Bill 17-438, March 11, 2007, *available at* http://epic.org/privacy/surveillance/epic_dc17-438_031108.pdf.

[2] Press Release, District of Columbia Mayor's Office, Mayor Fenty Launches VIPS Program; New System Will Consolidate City's Closed-Circuit TV Monitoring, Apr. 8, 2008, *available at* http://www.dc.gov/mayor/news/release.asp?id=1273&mon=200804.

[3] *Id*.

[4] *Id*.

[5] Letter from Darrell L. Darnell, Dir., D.C. Homeland Sec. and Emergency Mgmt. Agency, to Phil Mendelson, Chairman, Comm. on Public Safety & Judiciary, Regarding Questions Related to the Proposed FY 2009 Budget for D.C. HSEMA, Apr. 4, 2008, *available at* http://www.dccouncil.washington.dc.us/budget/Fiscal%20Year%202009%20Committee%20Questions%20and%20Answers/Committee%20on%20Public%20Safety%20and%20the%20Judiciary/PSJ%20FY09%20Responses/HSEMA.doc.

[6] Mary Beth Sheridan, *D.C. Will Centralize Security Monitoring*, WASHINGTON POST, Apr. 10, 2008.

[7] The Fair Information Practices were developed in the U.S. in 1973, and most countries follow the practices described by the OECD's 1980 Guidelines. U.S. Dep't. of Health, Educ. & Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *Records, Computers, and the Rights of Citizens* viii (1973), *available at* http://epic.org/privacy/consumer/code_fair_info.html; Org. for Econ. Cooperation & Dev., Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data, OECD Doc. 58 final (Sept. 23, 1980), art. 3(a), *available at* http://www.oecd.org/document/18/0,2340,es_2649_34255_1815186_1_1_1_1,00.html.

[8] Mike Dorning, *U.S. Cities Focus on Spy Cameras*, CHICAGO TRIBUNE, Aug. 8, 2005; Matthew Cella, *Spy Cameras Fail to Focus on Street Crime*, WASHINGTON TIMES, Aug. 13, 2006.

[9] Brent Champaco, *Cameras catch kiss, raising questions*, NEWS-TRIBUNE (Tacoma, Wash.), Apr. 26, 2007.

[10] Shaila K. Dewan, *Video of Suicide in Bronx Appears on Shock Web Site*, NEW YORK TIMES, Apr. 1, 2004.

[11] *Id*.

[12] *Id*.

[13] *Id*.

[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 (ChainLinks 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.

[17] 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.

[18] 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.

[19] 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 with Melissa Ngo).

[20] Metropolitan Police Dep't, *Closed Circuit Television (CCTV) Annual Report 2007* (Feb. 2008), *available at* http://mpdc.dc.gov/mpdc/frames.asp?doc=/mpdc/lib/mpdc/publications/CCTV_annual_report_2007.pdf.

[21] *Id*. at 9-10.

[22] *Id*. at 7.

[23] Mary M. Cheh, Chairperson, *Public Hearing*, Committee on Public Services and Consumer Affairs, D.C. Council, Mar. 11. 2008 (agenda *available at* http://dccouncil.us/calen95.htm).