November 13th, 2007

Toby Milgrom Levin
Department of Homeland Security
Washington, DC 20528
Fax: 703-235-0442

Mr. Levin:

Your so-called "privacy workshop" is merely the Delphi Method in sheep's clothing to manufacture consent for an Orwellian future that America doesn't want.

DHS has given millions of dollars to communities to build surveillance infrastructures primarily to socialize, acculturalize, and docilize American schoolchildren into accepting and obeying the techno-fascist machinery of a police-state future.

The following homeland security public servants abused me at the Texas border, at the Bridge of the Americas in El Paso, while also interfering with my Constitutional right to videotape them:

Neatherlin, Herrerra, Thome, Ortega, Blanco, Quintana, Moreno, Lopez, Martinez, Velaquez, Tarin, Menendez, Balderama.

Ysleta bridge offenders:
Labombarbe, Gomez, Pedroza, Madrid, Monahan, Jordan, Reed, Wolfe

ICE, CBP offenders:
Guillermo Rojas, J.J. Soto.

These people dressed and acted like Nazis running a concentration camp, and they swarmed me, and intimidated me, and threatened repeatedly to arrest me merely for attempting to lodge complaints about them, or as I was remaining silent, within my Constitutional rights.

DHS, you have disgraced the United States, and since you like CCTV so much, I look foward to videotaping your abusive employees as I cross the border into the United States, and I have no intention of putting the camera down.

We are sick of your abuse, we are sick of your lies, and you are violating and subverting the most sacred and important of human values and laws that have been developed over literally hundreds of years.

I invoked the 3rd Geneva Convention, and you said that I didn't have any rights. On a daily basis, you violate state constitutions, the US Constitution, federal statutes, city laws, county regulations, civil rights, common law rights, and international treaties--I mean, there are no literally no laws left for you Nazis to break, are there?

You try to frame people for pretended offenses (like brushing past an officer is assault, but you can break my neck or torture me, and it's either "necessary force", or "pain-compliance", respectively), and you literally send swarms of officers to harass the people. When I tried to gather video evidence against you, for the FBI and prosecutors, you attacked me and my camera, and then pre-positioned yourselves to lie in unison in court--you might vaguely remember such charges: they're found in the Declaration of Independence.

I guess it wouldn't have mattered if they had cameras back then, either, would it?

The President's signing statements and unreasonable, contortionistic interpretations are unlawful; they will not protect you from incurring civil and criminal liability.

See you at the border--my name is Jonathan Patrick Bazemore, I don't need to hide behind a numberless badge, or continuously shifting alphabet-soup acronym agencies that are continually dissolved and re-constituted to evade responsibility for their criminal behavior and institutionalized lawbreaking--remember to smile for my cameras, because the more you abuse us, the more resilient we will become, and we will never give up.

We haven't forgotten the concentration camps--and we won't let you forget it, either. Out of honor to those people who survived the camps, we won't allow you to repeat the mistakes of history, on this side of the Atlantic.

Sincerely,

Jonathan P. Bazemore.

November 30, 2007

Ms. Toby Milgrom Levin
U.S. Department of Homeland Security
400 Seventh Street, S.W.
Washington, D.C. 20528

Re: Comments to Docket No. DHS-2007-0076

Dear Ms. Levin:

The Washington Metropolitan Area Transit Authority (WMATA) is the largest mass transit provider in the Washington, D.C. metropolitan area and the second largest subway (rapid transit) and fifth largest bus system nationally. On average, we provide 720,000 rail trips, 439,000 bus trips, and 4,400 paratransit trips every weekday. WMATA uses closed circuit television (CCTV) cameras for safety, risk management and security purposes in its Metrorail rapid transit stations and on some of its Metrobuses, and is pleased to provide the following comments on Topic for Comment #5 regarding "the privacy and civil liberties best practices" (at 72 FR 63918).

While CCTV coverage of public areas generally carries no expectation of privacy, the appropriate uses of any resulting tapes should be considered. There is no question that the government may properly make use of the CCTV images, but the Department of Homeland Security (DHS) should consider whether those images should, as a matter of course, be releaseable to anyone who requests them. There must be a balancing of both public and privacy interests. In some cases, the public's interest may prevail, while in other cases, a person's privacy interest may be more important. We suggest that DHS consider making the establishment of a policy that covers both privacy interests and a records release policy a "best practice" for the use of CCTV.

We commend DHS on its efforts to develop privacy and civil liberties best practices and appreciate the opportunity to comment on this important issue.

Sincerely,

Deborah S. Lipman

Deborah S. Lipman
Director, Office of Policy and Intergovernmental Relations

Washington
Metropolitan Area
Transit Authority

600 Fifth Street, NW
ashington, DC 20001
202/962-1234

By Metrorail:
diciary Square—Red Line
allery Place-Chinatown—
Red, Green and
Yellow Lines
By Metrobus:
Routes D1, D3, D6, P6,
70, 71, 80, X2

*A District of Columbia,
Maryland and Virginia
Transit Partnership*

CCTV: Developing Privacy Best Practices
Privacy Office, Department of Homeland Security
Docket number: DHS-2007-0076.
James A. Lewis, January 9, 2008

CCTV use can improve security in urban areas, public venues, and around critical infrastructure facilities. The benefits of CCTV use will increase as the technology improves if we do not create a regulatory environment that discourages innovation and use. Privacy guidelines must be flexible enough to accommodate next-generation systems and evolving technologies and should not restrict further technological development.

CCTV is itself an anachronistic term. Old-style CCTV systems – a guard sitting in front of a screen or assembly of screens – will be replaced by automated, digital systems that use computer processing, digital networks and ubiquitous connectivity. In the near future, for example, a computer-controlled sensor will be able to track a vehicle that repeatedly circles a nuclear power plant, identify that vehicle's license number, automatically check that number and alert police or security forces if there is a concern.

CCTV use has grown rapidly because it provides benefits for security. Claims that CCTV does little to improve security should be contrasted with operational experience. When intelligence agencies describe a 'hard target' – e.g. a target where it is difficult to obtain access – the presence of surveillance cameras is one of the factors that makes the target hard. Covert access and the commission of illicit activities are made more difficult and riskier when CCTV surveillance is present. Denigrating the technology as a way to discourage its use should not be confused with a realistic appraisal of its utility.

The experience of other countries' CCTV use suggests that the presence or absence of CCTV is irrelevant to civil liberties. Civil liberties and political freedoms in China are restricted not because CCTV is in use, but because freedoms are generally restricted. In the UK, for example, the widespread use of CCTV has not damaged political freedoms. The effect of CCTV on civil liberties depends entirely on the larger political context. Democracies that have deployed CCTV in large numbers have not seen a chilling political effect.

Safeguards for CCTV should focus on how data that is collected or accessed by government agencies will be used, stored, and shared. Congress and the Courts have not dealt with this issue, although the laws governing search and seizure or wiretaps offer some precedent. There are significant differences however, between CCTV and wiretapping. The central issue is the status of images taken in public spaces. We expect telephone conversations to be private. Actions taken in the public view, where there is no reasonable expectation of privacy, are not private; they are in the public domain. Current laws impose some limits on monitoring. I cannot trespass or intrude ("objectionable intrusion") in collecting data. The data collected cannot be used for commercial or trade purposes (such as an advertisement) without my consent. And if the collector is from the police or another government agency, I cannot be subjected to an "unreasonable search."

The courts have not yet determined what is unreasonable. Is it an unreasonable search, for

example, if a camera mounted on a police cars can connect wirelessly to police computers running software that can identify a person with an outstanding warrant when that person is walking down the street? That person has no reasonable expectation of privacy, but instead relies on the likelihood that police officers he or she encounters will not know him or her. The use of CCTV can increases the knowledge and situational awareness of the police. Courts have restricted the ability of police to use sensors to look into a house (where there is a reasonable expectation of privacy), but appear open to the monitoring of public spaces.

This suggests that for the monitoring of open spaces or government-owned areas, there should be few constraints on collection and on use by the collecting agency. Retention of data should be for some publically specified and reasonable period. Sharing by the collecting agency with other government agencies s a more complicated issue. At a minimum, however, the shared data should be subject to the same constraints on retention, oversight and notification as apply at the collecting agency.

Changes in CCTV technology are part of a larger transition to a digital environment created by where cheap sensors, abundant processing and storage, and pervasive wireless networks. In this environment, privacy guidelines should focus on how bits are used or stored, not on how they are collected. Privacy guidelines for CCTV should build on public domain and a reasonable expectation of privacy. We should not expand privacy safeguards simply because the collector is a sensor rather than a human. Privacy guidelines address data retention and use. A framework for privacy rules governing CCTV use should consist of the following:

- No limits on collection of visual beyond what is currently required for visual surveillance in public spaces, government-owned spaces, or private spaces where the owner has agreed to allow video surveillance (collection of other kinds of imagery.

- A specified period for retention that is sufficient for law enforcement purposes.

- Clear public notice that CCTV surveillance is taking place.

- Published rules for the dissemination and use of CCTV data by the collector that also apply to third parties with whom such data is shared.

- The right to see photographic evidence if it is used in any legal action.

- Oversight by a body external to the collecting agency and public reporting on use.

- Rules for retention of CCTV data that are consistent with the treatment of similar kinds of government-collected data.

- Rule-making must accommodate the blending of different kinds of sensor data with CCTV data.

# COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

TO

# DEPARTMENT OF HOMELAND SECURITY

ON

## DOCKET NO. DHS-2007-0076
## NOTICE OF PRIVACY WORKSHOP AND REQUEST FOR COMMENTS

---

JANUARY 15, 2008

TABLE OF CONTENTS

# I. Introduction

By notice published on November 13, 2007, the Department of Homeland Security's Privacy Office announced a public workshop, "CCTV: Developing Privacy Best Practices," and requested comments on the topic.[1] The Privacy Office seeks "[t]o develop a comprehensive record regarding best practices for closed circuit television systems ("CCTV")."[2] Pursuant to this notice, the Electronic Privacy Information Center ("EPIC") submits these comments to detail a privacy framework that should be used if camera surveillance systems are to be created.[3]

EPIC has extensive expertise in surveillance issues, including those connected with camera systems. 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.[4] 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 original proposal.[5] In 2006, EPIC submitted detailed comments when the Metropolitan Police Department sought to

[1] Dep't of Homeland Sec., Notice Announcing Public Workshop, 72 Fed. Reg. 63,918 (Nov. 13, 2007) [hereinafter "DHS Notice About CCTV Workshop"], *available at* http://edocket.access.gpo.gov/2007/E7-22127.htm.
[2] *Id*.
[3] For general information about CCTV and privacy, *see* EPIC, Video Surveillance, http://epic.org/privacy/surveillance/.
[4] http://www.observingsurveillance.org/introduction.html.
[5] *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) [hereinafter "EPIC Testimony to D.C. Council"], *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.

dramatically expand the District's CCTV system.[6] That same year, EPIC testified about issue before the Department of Homeland Security Security's Data Privacy and Integrity Advisory Committee.[7] In December 2007, EPIC presented its proposed best practices for CCTV use at the Department of Homeland Security's Privacy Office workshop on camera surveillance systems.[8]

Camera surveillance networks are proliferating in cities across the country, even though studies conducted by government and independent organizations show that such systems have little effect on crime.[9] In fact, studies have found that it is more effective to place more officers on the streets than have them watching people on monitors.[10] For this, and many other reasons, EPIC believes that camera surveillance systems should not be used, current CCTV systems should be dismantled, and that funds for such systems should be allocated to more proven forms of crime prevention.

Since its creation in 2003 through December 2006, the Department of Homeland Security ("DHS") has allocated $230 million in grants for the creation and maintenance

---

[6] EPIC, *Comments to the Metropolitan Police Department for the District of Columbia on the Expansion of CCTV Pilot Program* (June 29, 2006) [hereinafter "EPIC Comments to D.C. Police"], *available at* http://www.epic.org/privacy/surveillance/cctvcom062906.pdf.

[7] *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) [hereinafter "EPIC Testimony to DHS"], *available at* http://www.epic.org/privacy/surveillance/coneytest060706.pdf.

[8] 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.

[9] 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.

[10] Home Office CCTV Study at vii, *supra* note 9; NACRO CCTV Study at 6, *supra* note 9.

of camera surveillance systems.[11] Millions more have been spent by states and localities.[12] If camera surveillance systems are to be used, then minimum security and privacy regulations need to be created to ensure strong protection of individual rights.

## II. Strong Privacy Frameworks Have Been Available for Decades

There is a history in the United States and internationally of protection of privacy rights. In 1948, the right of privacy was adopted into the Universal Declaration of Human Rights. Article 12 states, "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."[13]

The 1973 Fair Information Practices ("FIPs")[14] and the 1980 Organization of Economic Co-operation and Development ("OECD") privacy guidelines have had a significant impact on privacy law and regulation in the United States and internationally.[15] The Privacy Act of 1974 incorporates the FIPs and includes portions

[11] E-mail from Toby Levin, Senior Advisor, DHS Privacy Office, to Melissa Ngo, Senior Counsel, EPIC, Nov. 28, 2007 (on file with EPIC).
[12] EPIC AND PRIVACY INT'L, PRIVACY AND HUMAN RIGHTS 85-87 (EPIC 2006) [hereinafter "EPIC Privacy and Human Rights Report"].
[13] United Nations, Universal Declaration of Human Rights, G.A. Res. 217A(III), U.N. GAOR, 3d Sess., U.N. Doc. A/810 (1948), art. 12, reprinted in reprinted in M. ROTENBERG, ED., THE PRIVACY LAW SOURCEBOOK 383 (EPIC 2004) [hereinafter "Privacy Law Sourcebook"].
[14] 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) [hereinafter "HEW Fair Information Practices"], *available at* http://epic.org/privacy/consumer/code_fair_info.html.
[15] 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) [hereinafter "1980 OECD Privacy Guidelines"], reprinted in Privacy Law Sourcebook at 395. Also, the United Nations Guidelines for the Regulation of Computerized Personal Files of 1990 recognize many of the same rights in information as the OECD Privacy Guidelines provide, providing in addition that "data likely to give rise to unlawful or arbitrary discrimination, including information on racial or ethnic origin, colour, sex life, political opinions, philosophical and other beliefs . . . should not be compiled." United Nations, G.A. Res. 45/95, Guidelines for the Regulation of Computerized Personal Files (Dec. 14, 1990), reprinted in PRIVACY LAW SOURCEBOOK at 434. The United States is a signatory to the 1980 OECD Guidelines, the 1990 UN Guidelines and the Universal Declaration of Human Rights.

that were later included in the OECD guidelines.[16] Also, it must be noted that, in 2003, the European Court of Human Rights issued a judgment holding that the disclosure of CCTV pictures by a public authority may constitute a violation of an individual's right to privacy under Article 8 of the European Convention on Human Rights.[17]

The Fair Information Practices outlined by the U.S. Department of Health, Education and Welfare's Advisory Committee on Automated Data Systems are:

1. There must be no personal data record-keeping systems whose very existence is secret;

2. There must be a way for an individual to find out what information about him is in a record and how it is used;

3. There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent;

4. There must be a way for an individual to correct or amend a record of identifiable information about him; and

5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.[18]

The OECD Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data are:[19]

1. Collection Limitation Principle: "There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject";

2. Data Quality Principle: "Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date";

[16] *See* discussion *infra*.
[17] European Court of Human Rights, Fourth Section, *Peck v. The United Kingdom*, Application No. 44647/98, Strasbourg (Jan. 28, 2003).
[18] HEW Fair Information Practices, *supra* note 14.
[19] The following principles are excerpted from 1980 OECD Privacy Guidelines, *supra* note 15.

3. Purpose Specification Principle: "The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose";

4. Use Limitation Principle: "Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [the Purpose Specification Principle] except:
   a. with the consent of the data subject; or
   b. by the authority of law";

5. Security Safeguards Principle: "Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data";

6. Openness Principle: "There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller":

7. Individual Participation Principle: "An individual should have the right:
   a. to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
   b. to have communicated to him, data relating to him
      i. within a reasonable time;
      ii. at a charge, if any, that is not excessive;
      iii. in a reasonable manner; and
      iv. in a form that is readily intelligible to him;
   c. to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and
   d. to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended";

8. Accountability Principle: "A data controller should be accountable for complying with measures which give effect to the principles stated above."

The Privacy Act of 1974 implements the 1973 HEW Code of Fair Information Practices. When it enacted the Privacy Act in 1974, Congress sought to restrict the amount of personal data that Federal agencies could collect and required agencies to be

transparent in their information practices.[20] In 2004, the Supreme Court underscored the importance of the Privacy Act's restrictions upon agency use of personal data to protect privacy interests, noting that:

> "[I]n order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary . . . to regulate the collection, maintenance, use, and dissemination of information by such agencies." Privacy Act of 1974, §2(a)(5), 88 Stat. 1896. The Act gives agencies detailed instructions for managing their records and provides for various sorts of civil relief to individuals aggrieved by failures on the Government's part to comply with the requirements.[21]

The Privacy Act is intended "to promote accountability, responsibility, legislative oversight, and open government with respect to the use of computer technology in the personal information systems and data banks of the Federal Government[.]"[22] It is also intended to guard the privacy interests of citizens and lawful permanent residents against government intrusion. Congress found that "the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies," and recognized that "the right to privacy is a personal and fundamental right protected by the Constitution of the United States."[23] It thus sought to "provide certain protections for an individual against an invasion of personal privacy" by establishing a set of procedural and substantive rights.[24]

The Privacy Act ensures:

- an agency must give individuals access to the accounting of disclosure of their records[25];

[20] S. Rep. No. 93-1183 at 1 (1974).
[21] *Doe v. Chao*, 540 U.S. 614, 618 (2004).
[22] S. Rep. No. 93-1183 at 1.
[23] 5 U.S.C. § 552a.
[24] *Id*.
[25] 5 U.S.C. § 552a(c)(3).

- any agency or individual to whom the records are disclosed must also receive "any correction or notation of dispute"[26];
- individual may request access to records an agency maintains about him or her[27];
- an agency must correct identified inaccuracies promptly[28];
- an agency must make notes of requested amendments within the records[29];
- an agency must ensure it only collects data "relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by Executive order of the President"[30];
- an agency must "collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs"[31];
- each individual must be informed whom the agency asks to supply information[32];
- an agency must publish a notice of the existence of records in the Federal Register, along with the procedures to be followed to obtain access[33];
- an agency must establish procedures to handle disputes between the agency and individual as to the accuracy of the records[34]; and,
- an individual may seek judicial review to enforce the statutory right of access provided by the Act.[35]

The history of privacy protection in the United States and abroad is clear, as evidenced by these guidelines. These three privacy frameworks must form the foundation of any regulation of CCTV systems.

[26] 5 U.S.C. § 552a(c)(4).
[27] 5 U.S.C. § 552a(d)(1).
[28] 5 U.S.C. § 552a(d)(2)(B), (d)(3).
[29] 5 U.S.C. § 552a(d)(4).
[30] 5 U.S.C. § 552a(e)(1).
[31] 5 U.S.C. § 552a(e)(2).
[32] 5 U.S.C. § 552a(e)(3).
[33] 5 U.S.C. §§ 552a(e)(4)(G), (e)(4)(H), (f).
[34] 5 U.S.C. § 552a(f)(4).
[35] 5 U.S.C. § 552a(g)(1).

## III. There Is an Expectation of Privacy in Public Spaces

EPIC has previously explained, in testimony and written submissions, that 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 strongly recommends against the creation or expansion of CCTV systems to allow continuous, general surveillance of the public.

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

[36] EPIC Testimony to D.C. Council, *supra* note 5; EPIC Comments to D.C. Police *supra* note 6; EPIC Testimony to DHS, *supra* note 7.
[37] EPIC Testimony to DHS, *supra* note 7.
[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*.

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 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 society 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 all jurisdictions to reject the use of CCTV for general surveillance purposes and reassess their approach to privacy to include these issues.

---

[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] EPIC Testimony to DHS, *supra* note 7.
[44] EPIC Testimony to D.C. Council, *supra* note 5.
[45] *Id*.
[46] *Id*.

## IV. CCTV Contains Unique Privacy and Security Risks

While laws and guidelines exist to protect individuals' privacy, it is critical that a strong privacy framework be put in place that explicitly governs the implementation of CCTV systems in the United States. Because of the significant potential for CCTV systems to invade individuals' privacy and undermine civil liberty protections, CCTV must be independently regulated to ensure strong security and privacy safeguards. The very nature of video surveillance creates a significant power imbalance. The individual cannot see the watcher. The watched do not know who is watching, what they are watching for, or how the data being recorded, stored or used. Camera operators, on the other hand, are anonymous and may find that they are in a position of power in which no one monitors their use of the powerful technology at their disposal. Along with the lack of transparency, there are serious concerns relating to data consolidation and data sharing with third parties. Such a dearth of information as to the purposes and reasons for CCTV, along with the lack of transparency in how the systems are controlled and used, creates a situation that is ripe for abuse and misuse if proper controls are not put in place.

### A. Imbalance of Power Allows for Voyeuristic and Discriminatory Abuse of Camera Systems

There are numerous documented incidents in which CCTV system operators have abused their powers to invade individuals' privacy and undermine their Constitutional and civil rights. Below, we detail several examples that illustrate the necessity of strong limitations on CCTV creation and use.

In 2006 in England, two CCTV operators used public surveillance cameras to record images of a woman's home, using the technology to record her undressing and

bathing.[47] At the 2004 Republican National Convention in New York City, a police helicopter equipped with an infrared camera was deployed to monitor protesters but instead filmed a couple's intimate romantic activity on their terrace.[48] The couple was shielded by plants and in complete darkness; the only reason that they were seen by the police was because the infrared camera was able to track their body heat. In 2005, a police officer used surveillance cameras to gaze at women's breasts and buttocks at the San Francisco International Airport.[49]

Beyond voyeurism, there is the documented risk of discrimination under camera surveillance. Studies show that 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]

Increasingly, there has been creation and use of camera surveillance systems in housing complexes. The city of Aberdeen in Maryland passed a law in October 2007 that empowers the police and city government to require new "residential, commercial or industrial development[s]" to install CCTV systems before the development is issued a building permit.[52] These cameras would be linked to police systems.[53] There are no guidelines for how to determine if developments would need cameras, but the crime deterrent purpose assumes CCTV implementation in "high risk for crime areas."[54] This

---

[47] *Peeping Tom CCTV Workers Jailed*, BBC News, Jan. 13, 2006. 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) [hereinafter "Ngo Chapter on CCTV Myths"].
[48] Mike Dorning, *U.S. Cities Focus on Spy Cameras*, Chicago Tribune, Aug. 8, 2005.
[49] Matthew Cella, *Spy Cameras Fail to Focus on Street Crime*, *Washington Times*, Aug. 13, 2006.
[50] *Id.* (citing Clive Norris & Gary Armstrong, Ctr. for Criminology & Criminal Justice, Univ. of Hull (UK), *The Unforgiving Eye: CCTV Surveillance in Public Space* (1997)).
[51] NACRO CCTV study at 6, *supra* note 9.
[52] Madison Park, *City passes camera law*, Baltimore Sun, Oct. 7, 2007.
[53] *Id*.
[54] *Id*.

could disproportionately affect the poor.

Some CCTV systems in London and in the U.S. have been modified so that operators can speak to individuals in the vicinity of cameras. In Washington, D.C., the "talking CCTV" cameras have been installed at private apartment complexes where security guards have used the cameras to harass residents of the building, issuing humiliating commands such as "Get your fat ass off the corner!" over the public loudspeakers attached to the cameras.[55] Such abuse is made possible by the imbalance of power between the watcher and the watched.

### B. Cameras Allow for Monitoring of Lawful, Peaceful Protests

In addition to the harassment of individuals and racial profiling of surveillance targets, CCTV has increasingly been used to record and monitor individuals engaged in constitutionally protected activities such as freedom of association and speech during legal and peaceful protests. There are several documented instances in which law enforcement officials have conducted surveillance on lawful protests.

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.[56] Other documents revealed that the FBI used aerial video surveillance to monitor the same pro-life demonstrations and the D.C. Metropolitan Police Department used aerial surveillance to monitor demonstration activity on Inauguration Day in 2001. The D.C. Metropolitan Police Department also conducted aerial surveillance of demonstration activity for which "downlink photos of

[55] Dave Jamieson, *Speaker of the House*, Wash. City Paper, July 7, 2006.
[56] Detailed in EPIC Testimony to D.C. Council, *supra* note 5.

coffins/demonstrators" were provided by the U.S. Park Police.[57] These incidents are in addition to the New York police department's surveillance of protesters during the 2004 Republican National Convention.[58]

Surveillance of such activities should not focus on the faces of individuals nor seek to identify them in other ways without an actual threat to public safety. This kind of surveillance could create a chill on legal, constitutionally protected First Amendment activities. Freedom of association is fundamental to our democratic experience. Social justice, environmental, religious, and political movements have their foundation in the freedom of individuals who share like beliefs to associate with one another.

## V. EPIC Framework for Protecting Privacy and Civil Liberties If CCTV Systems Are Contemplated

We must reiterate that EPIC does not endorse nor support the creation of new or continued use of current camera surveillance systems, because their poor record on crime prevention does not outweigh the danger to privacy and civil liberties. However, if CCTV systems are contemplated, then they should follow the framework outlined below in order to ensure strong protections for privacy and civil rights.

### A. EPIC Guideline 1: CCTV Alternatives Preferred

**EPIC Guideline 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.

[57] *Id*.
[58] *See* discussion, *supra* Section III. A. Imbalance of Power Allows for Voyeuristic and Discriminatory Abuse of Camera Systems.

### B. EPIC Guideline 2: Demonstrated Need

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

### C. EPIC Guideline 3: Public Consultation

**EPIC Guideline 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.

### D. EPIC Guideline 4: Fair Information Practices

**EPIC Guideline 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.

### E. EPIC Guideline 5: Privacy Impact Assessment

**EPIC Guideline 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.

### F. EPIC Guideline 6: Enhanced Safeguards for Enhanced Surveillance

**EPIC Guideline 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 Federal Register notice request for comments, the Department of Homeland Security Privacy Office requested answers to five questions. EPIC will detail its answers within the privacy framework outlined above.

## VI. Numerous Jurisdictions and Organizations Have Detailed Best Practices for the Use of CCTV Systems

*Question 1: Are there existing state, local or international programs that have developed privacy or civil liberties guidelines for CCTV that can serve as resources for the development of best practices?*[59]

Domestic and international governments have detailed legislation and regulation of CCTV systems. Guidelines have been proposed by such domestic government agencies as Washington, D.C.'s Metropolitan Police Department ("MPD"),[60] and the federal

[59] 72 Fed. Reg. 63,918, *supra* note 1.
[60] D.C. Council, Metropolitan Police Department Video Surveillance Regulations Emergency Act of 2002, Act 14-302 (Mar. 25, 2002), *available at* http://dccouncil.washington.dc.us/images/00001/20020314161451.pdf.

National Park Service,[61] and non-profit non-governmental organizations such as EPIC and the Constitution Project.[62]

Internationally, Canadian federal and provincial privacy commissioners passed guidelines to help define and circumscribe the use of this medium and minimize its impact on privacy.[63] In Britain, the Information Commissioner's Office released guidelines in September 2002 and made a fresh call for revised guidelines in August 2007.[64] The Article 29 Data Protection Working Party also released guidelines for processing personal data by means of video surveillance.[65] The central premise of all of these guidelines is the belief that video surveillance poses unique threats to privacy and consequently requires unique controls to guard against its abuse.

---

[61] The federal National Park Service released guidelines in response to a March 2002 United States Congress hearing on video surveillance. *See Controversy Grows over Police Video Surveillance*, CNCNews.com, Mar. 22, 2002.

[62] Constitution Project, *Guidelines for Public Video Surveillance: A Guide to Protecting Communities and Preserving Civil Liberties* 10-13 (2006) [hereinafter "Constitution Project Guidelines"], *available at* http://www.constitutionproject.org/pdf/Video_Surveillance_Guidelines_Report_w_Model_Legislation4.pd.

[63] Office of the Privacy Comm'r of Canada, *OPC Guidelines for the Use of Video Surveillance of Public Places by Police and Law Enforcement Authorities* (Mar. 2006) [hereinafter "Canadian Privacy Commissioner CCTV Guidelines"], *available at* http://www.privcom.gc.ca/information/guide/vs_060301_e.asp. *See also* Gov't of British Columbia (Canada), *Privacy Guidelines for Use of Video Surveillance Technology by Public Bodies* (2004) [hereinafter "British Columbia CCTV Guidelines"], *available at* http://www.lcs.gov.bc.ca/privacyaccess/main/video_security.htm; Info. & Privacy Comm'r of Ontario (Canada), *Guidelines for Using Video Surveillance Cameras in Public Places* (Sept. 2007), *available at* http://www.ipc.on.ca/images/Resources/video-e.pdf; Office of the Info. & Privacy Comm'r for British Columbia (Canada), *Public Surveillance System Privacy Guidelines* (Jan. 26, 2001), *available at* http://www.oipcbc.org/advice/VID-SURV(2006).pdf.

[64] Press Release, Info. Comm'r's Office, ICO launches CCTV code of practice consultation, Aug. 29, 2007, *available at* http://www.ico.gov.uk/upload/documents/pressreleases/2007/determining_what_is_personal_data_press_release_final.pdf. *See also* Info. Comm'r's Office, *Data Protection Act 1998: Compliance advice CCTV Small User Checklist* (Sept. 2002), *available at* http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/cctv_small_user_checklist.pdf.

[65] *See* Article 29 Data Protection Working Party, *Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance* (Feb. 2004) [hereinafter "Article 29 Working Party Opinion on CCTV"], *available at* http://www.datenschutz-berlin.de/doc/eu/gruppe29/wp89/wp89_en.pdf. The report sets out guidelines under the EU Data Protection Directive in relation to surveillance by video cameras in public and work places.

In response to Question 1, we will detail how EPIC's privacy framework for CCTV use is reflected in the guidelines previously mentioned and are representative of the inter-jurisdictional consensus on what is required in order to make CCTV compliant with fair information practices and civil liberties protections.

### A. CCTV Should Be the Last Choice, Not the First

**EPIC Guideline 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.

A number of guidelines dictate that CCTV systems should not be used indiscriminately. For example, the Office of the Privacy Commissioner of Canada says, "less privacy-invasive alternative ways of addressing the identified problem should be chosen unless they are not feasible or significantly less effective."[66]

Germany's Federal Data Protection Act ("BDSG") regulates video surveillance.[67] Section 6b, "Monitoring of publicly accessible areas with optic-electronic devices," states that such surveillance is "allowable only in so far as it is necessary: 1) to fulfill public tasks, 2) to exercise the right to determine who shall be allowed or denied access or 3) to pursue rightful interests for precisely defined purpose," "and if there are no indications that the data subjects' legitimate interests prevail."[68]

### B. If CCTV Is Created To Solve a Problem, Then That Problem Must Be Explained Clearly to the Public

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

---

[66] Canadian Privacy Commissioner CCTV Guidelines, *supra* note 63. *See* British Columbia CCTV Guidelines, *supra* note 63.
[67] Germany, Federal Act on Data Protection ("BDSG"), Jan. 14, 2003 (*Bundesgesetzblatt*, Part 1, No 3, Jan. 16, 2003).
[68] Privacy and Human Rights Report at 92, *supra* note 12.

The Constitution Project, a non-profit non-governmental organization, has created a framework for privacy and civil liberties protection with CCTV systems. The first "step in the creation of a public video surveillance system is a clear statement of the legitimate law enforcement purpose and purposes for the system," the Constitution Project says.[69] The Privacy Commissioner of Canada held that "CCTV systems should only be deployed to address a clearly articulated problem that is real, pressing and substantial." The Privacy Commissioner requires that concrete evidence in the form of verifiable reports of the risks, dangers, and crime rates must be adduced to "warrant overriding the right of innocent individuals to be free from surveillance in a public place."[70]

### C. The Public's Voice Must Be Heard

**EPIC Guideline 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.

Public consultations ensure that the process remains transparent. The Department of Homeland Security emphasizes the importance of "transparency and analysis of privacy issues" in its "Official Guidance" for PIAs. The guidance document states that transparency demonstrates the Department's commitment to **"**privacy during the development of programs and systems and thus upholds the Department's commitment to maintain public trust and accountability. Without the trust of the public, the Department's mission is made more difficult."[71]

---

[69] Constitution Project Guidelines at 10-13, *supra* note 62.
[70] Canadian Privacy Commissioner CCTV Guidelines, *supra* note 63. *See also* British Columbia CCTV Guidelines, *supra* note 63.
[71] Privacy Office, Dep't of Homeland Sec., Privacy Impact Assessments Official Guidance (May 2007) [hereinafter "DHS Guidance on PIAs"], *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_guidance_may2007.pdf.

Further, under Section 208 of the E-Government Act, the DHS is required to conduct PIAs for all new or substantially changed technology that collects, uses, disseminates, or maintains personally identifiable information.[72] Any change in the technology used in CCTV systems would constitute such a change, thus requiring the governing authority to conduct fresh privacy impact analysis of the technology.

The public voice is prized internationally, as well. The Privacy Commissioner of Canada notes that "Community" should be understood broadly as being made up of several distinct communities, some of which might be disproportionately affected, and one "community should not be presumed to speak for the others."[73]

### D. Strong Privacy Frameworks Are Needed

**EPIC Guideline 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.

The Asia-Pacific Economic Cooperation ("APEC") Privacy Framework emphasizes the importance of collection limitations, uses of personal information, choice, and accountability and security safeguards.[74] The European Union Article 29 Data Protection Working Party document, "Working document on the processing of personal data by means of video surveillance," states that the information retention must be "quite short and in line with the specific features of the individual case."[75]

The need to adhere to FIPs is reflected in the guidelines required by the Canadian Privacy Commissioner, who emphasized that information collected through video

[72] *Id.* at 6.
[73] Canadian Privacy Commissioner CCTV Guidelines, *supra* note 63.
[74] Asia-Pacific Econ. Cooperation, *APEC Privacy Framework* (Oct. 2004), reprinted in Privacy Law Sourcebook at 512, *supra* note 13.
[75] Article 29 Working Party Opinion on CCTV at 20, *supra* note 65.

surveillance should be minimal, its use should be restricted, its disclosure controlled, its retention limited, and its destruction assured.[76] The Privacy Commissioner also highlights that the security of the equipment and images should be assured.[77]

One example of a U.S. agency applying the OECD framework is the Government Accountability Office's ("GAO") 2005 review of the Secure Flight travel program.[78] The GAO "used the eight Fair Information Practices proposed in 1980 by the Organization for Economic Cooperation and Development and that were endorsed by the U.S. Department of Commerce in 1981. These practices are collection limitation, purpose specification, use limitation, data quality, security safeguards, openness, individual participation," and accountability and stated that these Fair Information Practices are "a set of internationally recognized privacy principles that underlie the Privacy Act."[79]

In its submission to the Washington, D.C. Metropolitan Police Department, EPIC highlighted that the use of CCTV for law enforcement purposes presents the potential for misuse or abuse.[80] To combat this risk, EPIC said that access to the system's controls and reception equipment, and to the images it captures, should be limited to persons authorized in writing.[81] Recordings should be securely held, and access within the organization limited to a need-to-know basis.[82]

---

[76] Canadian Privacy Commissioner CCTV Guidelines, *supra* note 63.
[77] *Id*.
[78] Gov't Accountability Office, *Secure Flight Development and Testing Under Way, but Risks Should Be Managed as System Is Further Developed,* GAO-05-356 (Mar. 2005), *available at* http://www.gao.gov/new.items/d05356.pdf.
[79] *Id*. at 55.
[80] EPIC Comments to D.C. Police, *supra* note 6.
[81] *Id.*
[82] *Id.*

### E. Privacy and Civil Liberties Must Be a Part of the CCTV System From the Beginning

**EPIC Guideline 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.

Earlier, we discussed the possibility that video surveillance could infringe upon free speech. This view is supported by the Constitution Project's privacy and civil liberties framework, which notes that public surveillance cameras can negatively impact individuals' right to freedom of speech and association given that they can give the government an "extensive record of what individuals say and read, and indicate with whom they associate."[83] This could have a potentially "chilling" effect on the ability or desire of individuals to engage in constitutionally protected conduct, according to the group.[84] As previously mentioned, the Department of Homeland Security emphasizes the importance of "transparency and analysis of privacy issues" in its Official Guidance for PIAs.[85]

### F. This Framework Does Not Preclude Stronger or Different Safeguard That May Be Necessary As Technology Changes

**EPIC Guideline 6: Enhanced Safeguards for Enhanced Surveillance:** Any additional surveillance and image analysis capabilities added to cameras or other technology will require corresponding privacy and security safeguards. Apply to any law enforcement use of privately collected CCTV data the same standards that apply to public CCTV data.

Given the ever-increasing sophistication of surveillance technology due to research and development, many jurisdictions have urged the need to conduct regular evaluations of the privacy impacts of new technology. Section 208 of the E-Government Act, requires DHS to conduct PIAs for all new or substantially changed technology that

[83] Constitution Project Guidelines at 18-19, *supra* note 62.
[84] *Id*.
[85] DHS Guidance on PIAs, *supra* note 71.

collects, uses, disseminates, or maintains personally identifiable information.[86] The United Kingdom's Information Commission Office has revised its existing code of practice on camera surveillance to reflect technological developments and changes to the way CCTV is used to monitor individuals.[87]

## VII. Privacy and Civil Liberties Protections Are Fundamental To Any CCTV System

*Question 2: How can CCTV systems be designed in a manner that respects privacy and civil liberties?*
*Question 5: What are the privacy and civil liberties best practices you would recommend for government use of CCTV?*
[These will be answered together.]

The best way to protect individual privacy rights and civil liberties is to enforce the EPIC Framework for Protecting Privacy and Civil Liberties If CCTV Systems Are Contemplated. These guidelines incorporate Fair Information Practices, the 1980 OECD Privacy Guidelines, and the Privacy Act of 1974, which are reflected in jurisdictions around the world and are well-established in domestic privacy law.

### A. Video Surveillance Should Not Be Undertaken Lightly

**EPIC Guideline 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.

Governments internationally and domestically are increasingly implementing CCTV systems to monitor their citizens despite the prohibitive cost of such technology and demonstrated inefficacy at reducing crime.[88] The Department of Homeland Security

[86] *Id*. at 6.
[87] Press Release, Info. Comm'r's Office, ICO launches CCTV code of practice consultation, *supra* note 64.
[88] Studies have found that such surveillance systems have little effect on crime, and that it is more effective to place more officers on the streets and improve lighting in high-crime areas. *See generally* Privacy and Human Rights Report at 85-98, *supra* note 12; Home Office Study, *supra* note 9; NACRO Study, *supra*

has given $230 million in grants to state and local governments,[89] such as Washington, D.C.,[90] New York, and Chicago,[91] to create networks of surveillance cameras to watch over the public in the streets, shopping centers, at airports and more. A number of other countries also have CCTV systems.[92] Great Britain has an extensive surveillance network. London alone has 200,000 cameras, and more than 4 million cameras have been deployed throughout the country.[93] China, Germany and Greece are among the countries with camera surveillance systems.[94]

By their very nature, CCTV systems invade the privacy of all individuals. The increasing deployment of CCTV means that people are remotely monitored and have their legal actions recorded and saved in more and more public locations and at more and more public events. Rather than expanding video surveillance systems to monitor each and every aspect of innocent individuals' public behavior, CCTV systems should be installed only as a last resort and only if it is demonstrated that alternative methods of achieving the same goal are ineffective or not feasible.

---

note 9. 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, supra *note 9*; Privacy and Human Rights Report at 85-98, *supra* note 12. In 2005, a Milwaukee study found that law enforcement officials in cities such as Detroit, Mich.; Miami, Fla.; and Oakland, Calif., abandoned the use of these surveillance systems because of poor results. *See* Ryan Davis, *Surveillance cameras may soon be coming to a street near you*, Baltimore Sun, Mar. 16, 2005. *See also* Al Swanson, *Analysis: Are video cameras aiding police?*, United Press Int'l, Feb. 25, 2005.

[89] EPIC has been following the growth in the use of such camera systems for several years, including the Washington, D.C., surveillance network. S*ee* EPIC, Spotlight on Surveillance, *More Cities Deploy Camera Surveillance Systems with Federal Grant Money* (May 2005), *at* http://www.epic.org/privacy/surveillance/spotlight/0505/.

[90] For an extensive examination of the prevalence and privacy implications of Washington, D.C.'s, CCTV system, *see* EPIC, Spotlight on Surveillance, *D.C.'s Camera System Should Focus on Emergencies, Not Daily Life* (Dec. 2005), *available at* http://epic.org/privacy/surveillance/spotlight/1205/.

[91] Fran Spielman, *Feds give city $48 million in anti-terrorism funds*, Chicago Sun-Times, Dec. 4, 2004.

[92] For more on the prevalence of public surveillance in Canada, *see* CIPPIC, Public Video Surveillance, http://www.cippic.ca/public-video-surveillance/.

[93] Fran Spielman and Frank Main, *City plans camera surveillance web*, Chicago Sun-Times, Sept. 10, 2004; s*ee generally* Privacy Int'l, Overview: CCTV and Beyond, http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-65433.

[94] Privacy and Human Rights Report at 85-98, *supra* note 12.

This guideline is required in order to prevent against the abuses and misuses of CCTV to record peoples intimate moments mentioned in the introduction. In addition to the harassment of individuals, invasion of their privacy and racial profiling of surveillance targets, CCTV has increasingly been used to record and monitor constitutional freedom of association activities, such as legal protests.[95] Freedom of association and expression are fundamental to our democratic experience.

In addition to creating situations in which individuals may have their privacy rights invaded in ways that were never before possible, CCTV systems are prohibitively expensive. Governments must be economically accountable to its citizens in addition to any form of rights based accountability. Given that taxpayers are funding the installation of such systems, their ability to deter crime must be demonstrated. It has not.[96] Money invested in video surveillance systems in American cities could be used to pay for more police officers, better street lighting, and public education about neighborhood safety and security. Traditional methods of policing are far less expensive and far more effective at creating safe communities than expensive CCTV video surveillance systems.

The social cost of videotaping public places and activities must be taken into account when doing a full cost-benefit analysis of proposed CCTV projects. The public must consider the risks for misuse or abuse through voyeurism or economic, social or racial discrimination. What is the cost to the community if CCTV surveillance makes individuals reluctant to exercise their civil rights, because they fear repercussion if they are unable to demonstrate anonymously? All costs must be considered in the decision to develop or expand a video surveillance system.

---

[95] *See* discussion *supra* Section II B. Cameras Allow for Monitoring of Lawful, Peaceful Protests.
[96] *See* discussion *supra* Section V. Numerous Jurisdictions and Organizations Have Detailed Best Practices for the Use of CCTV Systems.

### B. There Must Be a Demonstrated Need for CCTV That Overcomes the Privacy and Civil Liberties Risks Created By Such Systems

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

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.

For example, many municipal CCTV systems are installed and funded on the belief that they will help to fight crime. However, studies conducted by government agencies in the U.S. and internationally have found video surveillance has little effect on crime rates.[97] 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.[98]

If the program goals have not first been clearly articulated, then there is no way to conduct a periodic review to determine whether CCTV is working to "fight crime" in a particular community. By clearly stating why CCTV is considered necessary and what problem it is attempting to prevent or correct, decision-makers then a basis by which to

[97] *See generally* Privacy and Human Rights Report at 85-98, *supra* note 12; Home Office Study, *supra* note 9; NACRO Study, *supra* note 9. 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, supra *note 9*; Privacy and Human Rights Report at 85-98, *supra* note 12.

[98] *See* Ngo Chapter on CCTV Myths, *supra* note 47.

measure the impact of the surveillance system on the community and decide if it is effective enough to warrant further or increased expenditure to maintain. Articulating a clear reason for the proposed video surveillance system allows members of the public and oversight bodies to hold decision-makers accountable if there is a failure of the system to achieve its purpose.

### C. Public Consultation Is Necessary for Public Acceptance

**EPIC Guideline 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.

CCTV affects every individual's right to privacy and anonymity as they go about their lives. CCTV systems that are installed by government agencies are paid for by taxpayer funds. Expenditure of public funds requires a transparent process in order to be politically legitimate and to increase public trust and confidence in the system.

In some cases, the very people being monitored are required to pay for their surveillance. New York City plans to partially finance its proposed "Ring of Steel" in Manhattan by imposing the costs on the drivers who enter the area.[99]

Public resources are limited, so the decision to spend $230 million in Homeland Security grants on camera surveillance systems means that money is no longer available to pay for more police officers or create social programs for communities.[100] Individuals, community groups, and privacy and security experts must have an opportunity to provide meaningful input into the decision-making process about whether the money can be put to more effective use elsewhere.

---

[99] Cara Buckley, *New York Plans Surveillance Veil for Downtown*, N.Y. Times, July 9, 2007, at A1; Tom Leonard, *'Ring of Steel' Plan to Protect New Yorkers*, Telegraph, July 10, 2007.
[100] E-mail from Toby Levin, *supra* note 11.

Decisions about whether or not to install CCTV systems are not limited to financial considerations. The public, local community groups, and privacy and security experts must also be given an opportunity to decide whether or the invasiveness of CCTV systems is a social cost that is worthwhile.

### D. Fair Information Practices Will Work to Protect Individual Rights Under CCTV Systems

**EPIC Guideline 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.

The ultimate goal of all CCTV surveillance systems is to create safe, well-functioning communities. Unfortunately, there have been many documented instances of abuse of CCTV surveillance systems and operators have been caught using the technology to discriminate against racial minorities, to single out women for sexual harassment and inappropriate observation, and to observe and record the identities of innocent individuals exercising their First Amendment rights to free speech and freedom of association.

Given the potential for abuse, individuals must know when they are monitored on CCTV systems, why the monitoring is taking place, and who has responsibility for gathering and storing the data. Making this information publicly available allows individuals to know if their privacy rights or civil liberties have been violated and gives them the opportunity to try to correct any misinformation or mistakes in the record or to

hold individuals accountable if they have been inappropriately and illegally targeted for surveillance.

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.

For reasons detailed above, it must be clearly explained to the public why a CCTV system is being implemented and what it is intended to achieve. Articulating a goal allows for thorough debate about whether it can be achieved by video surveillance or if a different technique would be better suited to solving the problem. This, in turn, allows for debate about how to spend limited public money most effectively.

It is also necessary to set clear, objective standards in order to allow regular independent audits of the system and whether it is achieving the articulated goal. If, after a periodic review the CCTV system is not found to be effective at achieving the purpose for which it was installed, then there must be a means of un-installing the system so that it does not continue to invade individuals' privacy or waste limited public resources.

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.

To minimize the risk of abuse or misuse of data collected and stored under CCTV systems, policies must be implemented that limit how much information is gathered and stored, as well as how long it is stored for. The data should only be kept for as long as is required to achieve the stated purpose of the video surveillance system and then destroyed.

Strict guidelines should be put in place to limit the number of individuals who have access to information in order to limit improper use of stored data. Limiting access to the system and the length of time that the data is stored minimizes the negative impact on constitutional rights when the CCTV system is properly used. It also reduces the possibility that the system will be misused, helping to reduce legal liability that is incurred if and when individuals improperly use CCTV to harass individuals or discriminate against certain sections of the population.

There are several ways in which data collection and retention can be minimized, including:

1. only operating the system for the length of time necessary to achieve its stated goal;
2. limiting the application of the CCTV system to the geographic area where the targeted problem exists and do not extend the system into neighboring areas in which there is no problem; and
3. refusing to add additional technological capabilities which may invade privacy but do not help to achieve the articulated goals of the CCTV system.

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.

There are a variety of ways in which CCTV systems may be abused, including criminal misuse of the data collected by individuals who have access to the information, institutional misuse by departments, discrimination against individuals, and voyeurism. Therefore, there must be an independent oversight office created in jurisdictions that implement CCTV systems. Giving an independent party the power to audit, investigate, and, if necessary, hold accountable CCTV system operators and officials ensures the protection of individuals. Routine audits by an independent oversight body with

enforcement capabilities will create more public trust in the CCTV system. Individuals and community organizations fears of the potential privacy and civil liberties abuses that can arise from the system's misuse would be allayed.

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.

Because of the potential for serious misuse of CCTV systems, individuals who are subject to video surveillance must have a way to hold individuals and departments who have misused the system legally responsible. Creating a private right of action for individuals will act as a deterrent to any individuals who may consider using a CCTV system improperly.

Databases are not foolproof and can often contain inaccurate information. Surveillance data that is stored is subject to the same concerns of inaccuracy, particularly if there are additional capabilities, such as facial identification. If the images are being checked against a database that contains errors, then innocent individuals might become the target of law enforcement investigations or other measures. Individuals must have a way to ensure that the data that is stored is accurate; otherwise, they may be subject to law enforcement measures based on faulty information.

The Privacy Act of 1974 creates a precedent for this type of accountability measure, because it allows private individuals to sue the government if it is not in compliance with the provisions of the Act.[101] Under the EPIC Framework for Protecting Privacy and Civil Liberties If CCTV Systems Are Contemplated, individuals would have

[101] 5 U.S.C. § 552a(d)(1), (f)(4) and (g)(1).

a right to sue if the government or government departments were not compliant with the established regulations governing CCTV.

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.

In situations in which CCTV surveillance data must be stored for any length of time, steps must be taken to secure the data so that it is not stolen or used for reasons other than its clearly articulated intended purpose. Security safeguards should include encryption and limiting access to stored data to persons with layers of clearance. Technological safeguards should be added creating audit trails that could demonstrate when and where information was accessed. This will act as a disincentive to any individual who may wish to use the information improperly and protect the system from mission creep.

Technical and institutional security measures must be verified by outside independent assessors and the results made publicly available to ensure that the security safeguards are adequate and do not contain any flaws that may compromise the security of the data that is stored or the privacy rights of individuals who may be captured on camera. Because of the potential for misuse of the CCTV system and the many documented cases of such abuse, individuals who work with the system must be regularly trained in privacy and civil liberties rights and regulations, and their work must be supervised to ensure that they do not engage in any such behavior.

**EPIC Guideline 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.

CCTV surveillance systems necessarily diminish individuals' privacy in that they record and store for potential review by strangers and system operators' public incidents that would not normally attract attention. CCTV systems and government surveillance in general has the potential to create a "chilling" effect on individuals' constitutionally protected rights such as the right to free speech and to freedom of association. If law enforcement is able to record what individuals say, where they spend their time, and with whom they associate, then individuals could become reluctant to exercise their First Amendment rights.

CCTV systems also have the potential to single out for further surveillance a particular segment of the population. In many documented cases, selection of individuals for further surveillance has been done along discriminatory lines and individuals have been monitored because they fit certain racial characteristics rather than because they were acting in a suspicious manner. For example, young black males are predominantly singled out for further surveillance.[102]

Because of the potential for negative impacts on civil liberties and privacy rights, a Privacy and Civil Liberties Impact Assessment must be conducted before it is decided that a CCTV system is the appropriate means of targeting a particular problem. Privacy Impact Assessments are already conducted before the implementation of many government projects. PIAs are an effective tool for determining what the exact privacy concerns are on any given issue. By adding in a requirement that, in the context of CCTV deployment, system operators must also consider the impact on civil liberties, Privacy and Civil Liberties Impact Assessments will be effective tools for determining whether CCTV is the appropriate means of targeting a particular problem, and such assessments

[102] Clive Norris & Gary Armstrong, *supra* note 50; NACRO Study, *supra* note 9.

help to achieve "transparency and analysis of privacy issues" as called for in the DHS' Official Guidance for PIAs.[103]

**EPIC Guideline 6: Enhanced Safeguards for Enhanced Surveillance:** Any additional surveillance and image analysis capabilities added to cameras or other technology will require corresponding privacy and security safeguards. Apply to any law enforcement use of privately collected CCTV data the same standards that apply to public CCTV data.

Best practices must recognize that the privacy invasiveness of CCTV is directly dependent on the sophistication of the technology employed. For example, CCTV technology that merely surveys a crowd is less invasive than technology that is equipped with face recognition software.[104] To be able to properly assess the privacy and civil liberties implications of technological changes to CCTV, there must be a new Privacy and Civil Liberties Impact Assessment in any situation where new CCTV technology is contemplated. By completing such an assessment, officials will be able to determine whether the more privacy-invading technology is the appropriate means to achieve the stated goal or whether a less privacy-invasive technique would be more effective. Also, there must be renewed discussion with the public about the potential privacy and security risks involved so that the public may make an informed cost-benefit analysis.

The protections outlined in the EPIC Framework for Protecting Privacy and Civil Liberties If CCTV Systems Are Contemplated should be applied to both public and private surveillance systems. In this way, the public is assured that their privacy and civil rights are being protected.

[103] DHS Guidance on PIAs, *supra* note 71.
[104] *See* EPIC, Face Recognition, http://epic.org/privacy/facerecognition/.

## VIII. Melding of Public and Private Data Creates Innumerable Privacy and Security Risks

*Question 3: What measures are necessary to protect privacy and civil liberties when governments have the ability to link into privately owned CCTV networks or have access to images and footage that such networks have captured?*[105]

### A. Private CCTV Systems Are Growing Rapidly

Video surveillance is being increasingly used by private actors for law enforcement type purposes. In a nationwide survey from as far back as 1996, more than 75 percent of companies surveyed utilized CCTV surveillance.[106] CCTV networks are employed by the private sector for a number of purposes, ranging from businesses monitoring their properties to the installation of nanny cams in private homes.[107]

### B. Private Video Surveillance Could Create Higher Privacy Risks

Public operators of CCTV systems are bound by procedural limits. Operators of private CCTV systems are not bound by any such limits. Currently, there is no uniform training requirement. Without strict regulation and training, such technology might be used by private parties to improperly monitor citizens and engage in discriminatory practices. Above, we detailed instances of CCTV abuse or misuse by public operators are regulated. It is unknown what the rate of abuse is in the private sector, where training is not required or ensured. Also, there are questions about "deputizing" commercial entities and what Fourth Amendment questions could arise from government entities retrieving such data without a warrant.

---

[105] 72 Fed. Reg. at 63,918, *supra* note 1.
[106] Karen Hallberg, Research Dir., Cahners Publ'g Co., *Nationwide Survey of Companies With Security Expenses* (Sept. 1996).
[107] *New Jersey v. Diaz,* 308 N.J. Super. 504 (App. Div 1998).

## IX. Current Privacy Impact Assessments Can Be Re-tooled to More Effectively Safeguard Individual Rights

*Question 4: How can Privacy Impact Assessments (PIAs) be used as a means of protecting privacy in this area? What would make for an effective PIA? How can government agencies incorporate the findings of PIAs into their CCTV networks and guidelines?*[108]

### A. Proper Balance Is Required

In balancing the privacy risks associated with such information consolidation, DHS has stated that it will put "in place robust protections for the privacy of any personally identifiable information that it collects, uses, disseminates, or maintains."[109] It has promised to meet the following three objectives: (1) Minimize intrusiveness into the lives of individuals, (2) Maximize fairness in institutional decisions made about individuals, and, (3) Provide individuals with legitimate, enforceable expectations of confidentiality.

DHS states that "PIA analyzes how personally identifiable information is collected, used, stored, and protected by the Department and examines how the Department has incorporated privacy concerns throughout its development, design, and deployment of a technology or rulemaking."[110] As discussed above, CCTV surveillance poses unique privacy risks due to the technology's ability to record continuous, detailed information about individuals and store the date for infinite replay and analysis.[111] In order to properly analyze the true privacy impact of CCTV surveillance, it is crucial that any PIA conducted account for these unique risks. The necessity for the government to take into account the unique privacy risks of any new technology or system is explicitly

[108] 72 Fed. Reg. at 63,918, *supra* note 1.
[109] DHS Guidance on PIAs, *supra* note 71.
[110] *Id.*
[111] For a discussion of the unique risks posed by CCTV technology, *see* discussion *supra* Section V. Numerous Jurisdictions and Organizations Have Detailed Best Practices for the Use of CCTV Systems.

set out in Section 208 of the E-Government Act. The E-Government Act further requires DHS to conduct PIAs for all new or substantially changed technology that collects, uses, disseminates, or maintains personally identifiable information.

### B. Specific Recommendations On How To Change Current PIAs To Apply Them To Video Surveillance Systems

Any PIA conducted to evaluate the privacy implications of a CCTV system must include the following:

#### i. A Clear Definition of Privacy That Encompasses the Dynamic and Intensely Detailed Nature of Continuous Video Surveillance

While the current definition of "information" privacy used in PIAs includes all information that is "personally identifiable," including facial images, it does not adequately capture the dynamic and intensely detailed information captured by CCTV. Information captured by CCTV systems is more akin to the "personal information" referred to in the Official Guidance as "private information." "Private information," DHS says, "is information that an individual would prefer not be known to the public because it is of an intimate nature."[112] As demonstrated by the abuses of public surveillance, such as infrared technology that allowed police officers to monitor a New York couple engaged in an intimate moment, CCTV technology captures precisely this data.

#### ii. Under the "Overview" Section, Government Agencies Must Explicitly State the Exact Purpose of the Use of CCTV Technology

Given the cost and unproven effectiveness of CCTV surveillance in decreasing crime (as detailed above), such a purpose requirement is imperative to ensure that the

[112] DHS Guidance on PIAs at 7, *supra* note 71.

program's efficacy can be properly evaluated. This should be added to the "Overview" section.[113]

### iii. Section 1.1 Must Specify the Nature and Extent of Information Sharing and Consolidation Between Databases

This limitation on the sharing of data collected is evident in many privacy frameworks. The Code of Fair Information Practices state that an individual "must be able to prevent information obtained about him for one purpose from being used or made available for other purposes without his consent."[114] The OECD Guidelines state "The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose."[115] The Privacy Act of 1974 requires that an agency must ensure it only collects data "relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by Executive order of the President."[116]

### iv. Sections 1.2 and 6.0 Must Indicate the Location of CCTV Cameras In Order To Ensure Proper Public Notice and Compliance With Fair Information Practices

If an individual does not know where his actions will be recorded, he has no way of finding out what information about him is contained within a record. This is necessary

[113] *Id* at 2.
[114] HEW Fair Information Practices, *supra* note 14.
[115] 1980 OECD Privacy Guidelines, *supra* note 15.
[116] 5 U.S.C. § 552a(e)(1).

for the notice, access and correction provisions of FIPs, the OECD Privacy Guidelines, and the Privacy Act of 1974.[117]

### v. Section 1.3 Must Include the Uses For Which the Information Is Employed Given That It Is Susceptible To Abuse, Specifically Looking At: (1) Abuse For Personal Purposes; (2) Criminal Abuse; (3) Institutional Abuse; (4) Discriminatory Targeting; and (5) Voyeurism

The FIPs, the OECD Privacy Guidelines, and the Privacy Act of 1974 all include provisions requiring that individuals know the purpose for data collection.[118]

### vi. Sections 1.4 and 2.0 Must Specify the Exact Nature of Images and Information Collected

This information is required in order to ensure consensus on limits CCTV systems. The video surveillance technologies allowing for zoom, audio, face recognition, heat detection, and motion-sensing would all need to be evaluated. Specifying the nature and extent of limits on camera use would help to prevent misuse and abuses. The FIPs, the OECD Privacy Guidelines, and the Privacy Act of 1974 all include provisions limiting the collection of data.[119]

### vii. Section 1.7 Must Include a Discussion of the Potential Impact the CCTV Technology Might Have on Civil Liberties

Above, we have thoroughly discussed the use of surveillance to monitor lawful, peaceful demonstration, which could chill free speech and association. This is just one of the many possible effects video surveillance could have on civil liberties, and such possible effects must be thoroughly analyzed.

---

[117] HEW Fair Information Practices, *supra* note 14; 1980 OECD Privacy Guidelines, *supra* note 15; 5 U.S.C. § 552a (1974).
[118] *Id.*
[119] *Id*.

### viii. Sections 4.0, 5.0 and 8.0 Must Include a Discussion of How Access to Records Will Be Limited At the Time the Information Is Gathered and During the Retention Period

Such limitations on access to CCTV data is crucial, given the ease of mission creep and abuse of the systems. For CCTV to retain public support, all opportunities must be taken to prevent against its abuse, misuse or flagrant expansion of its use.

### ix. Section 7.0 Must Be Changed to Include a Means of Reviewing the Program's Efficacy and Operational Privacy Impact

The Privacy and Civil Liberties Assessment of any proposed video surveillance system must include an examination of the operational extent and nature of the information's use, as well as the extent of the data retention. There must also be a process for timely independent review of the program with public disclosure of such assessments.

## X. Conclusion

In order to establish public trust in the surveillance operations of government, 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 as it strengthens political legitimacy of government control. The application of CCTV technology by law enforcement or private companies should not be excluded from transparency objectives.

Any creation or expansion of CCTV systems would have serious privacy implications; therefore, strong regulations, oversight, and penalties must be adopted in parallel to prevent abuses and protect the public's privacy and civil rights. EPIC does not support the creation nor the expansion of video surveillance systems, because their limited benefits do not outweigh their enormous monetary and social costs. EPIC urges

the DHS not to encourage the expansion of such systems. If, however, CCTV systems are contemplated, EPIC recommends that DHS implement its proposed Framework for Protective Privacy and Civil Liberties If CCTV Systems Are Contemplated: (1) video surveillance should be viewed as an exceptional step, only to be taken in the absence of a less privacy invasive alternative; (2) CCTV systems should only be deployed to address a clearly articulated problem that is real, pressing, substantial; (3) the public, local community, 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) the use of video surveillance should be governed by an explicit policy based on Fair Information Practices; (5) before implementing any CCTV system, conduct a privacy and civil liberties assessment to detail how such a system could effect Constitutional rights and civil liberties; (6) any additional analysis capability added by "smart" cameras or other technology will require corresponding privacy and security safeguards.

The proposed framework mirrors those implemented in many jurisdictions domestically and internationally. All such guidelines recognize the unique privacy concerns raised by public surveillance technology that is marked by an imbalance of power between the government as "watcher" and the citizens as "subject." The proposed guidelines help to make an otherwise opaque law enforcement mechanism more transparent in order to better protect privacy rights and civil liberties.

Respectfully submitted,

_____

Melissa Ngo
Senior Counsel

CCTV Workshop Comment: DHS-2007-0076

# You Better Watch Out, You Better Not Frown, New Video Surveillance Technologies are Already in Town (and Other Public Spaces)

*Draft Version*
Scheduled for publication in the Winter 2008 issue of
*I/S: A Journal of Law and Policy for the Information Age*

CARLA SCHERR*

ABSTRACT

*The use of video surveillance systems to capture images of Americans in public and pseudo-public spaces has grown faster than privacy law's ability to respond. New technologies and security concerns have revolutionized the way video-surveillance images are captured, stored, and transmitted, and raise arguments that the subjects of such monitoring should have some right to control the use of those images. Because the monitored spaces are public, existing privacy law neither protects persons under surveillance nor acknowledges a need for such protection; therefore, the existing factors used to assess the reasonableness of an expectation of privacy are not appropriate to the new technologies. New factors should be developed in response to the capabilities of the new technologies, so that privacy laws addressing these technologies are thoroughly evaluated. These factors should include the distance between the camera and the subject and the degree of magnification employed; whether specific individuals are selected and tracked; whether individual subjects are identified; the durability and*

* Carla Scherr is a juris doctor candidate at The Ohio State University Moritz College of Law, class of 2008. She received a B.A. in Mathematics from Wellesley College in 1984 and a B.S. in Earth, Atmospheric and Planetary Sciences from the Massachusetts Institute of Technology in 1985.

*distribution of the images; the likelihood of unauthorized image use and modification; and whether images are correlated with data from other sources.*

## INTRODUCTION

Privacy laws that address surveillance through the capture of visual images have traditionally relied on an analogy between actions visible to passers-by and actions captured by cameras. New surveillance technologies have rendered this analogy inapplicable; there is a difference between a passer-by and a video surveillance camera. A passer-by's observation is restricted to what can be seen by the naked eye. The passer-by can, of course, use vision-enhancing equipment, such as binoculars, but since the passer-by exists in the same time and space as the subject, the subject is likely to know of the observation and to have an opportunity to react. The subject of video surveillance, however, is not likely to know that he or she is being watched, what type of image is being captured, who is reviewing the image and where he or she is located, when the image is being reviewed, or how the image is being modified.

The past few years have seen tremendous advances in video surveillance technologies, as well as drastic decreases in the cost of those technologies. As a result, there has been an explosion in the use of video surveillance. At the same time, we have seen unprecedented changes in our society's security situation and attitudes towards privacy and public spaces. What we have not seen is corresponding changes in the privacy laws concerning video surveillance of public spaces.

Neither the Constitution nor the Bill of Rights specifically mentions a right to privacy. As a result, the conditions under which a person has a legitimate right to privacy are defined in much the same way as pornography, by using the "I'll know it if I see it" sniff test. Video

surveillance of public spaces avoids all of the traditional tests used to establish a legitimate expectation of privacy. Thus there is no legal tripwire to protect citizens from unwanted video image capture by either state or private actors. There is a gut feeling, nevertheless, that some right to control the use of one's image exists, even if the image was captured in a public space.

Until recently, society had neither the technology nor the desire to engage in detailed, wholesale visual surveillance of its public spaces. After the terrorist attacks of 9/11, however, our technology and our awareness of security issues matured quickly. We are now blessed, or perhaps cursed, with both the ability and the desire to watch and record the actions of our fellow citizens at a level of detail that raises new privacy issues and compels us to re-examine our expectations of privacy in the context of video surveillance of public spaces. The definition of a legitimate expectation of privacy, like the definition of pornography, must keep pace with changes in society and technology.

This Note identifies factors that should be considered in assessing the adequacy of existing privacy law as applied to video surveillance of public spaces by private entities. The Note restricts its consideration to situations where there is neither audio capture nor suspicious behavior by the subjects of the surveillance. Part I discusses recent developments in technology and society that postdate the establishment of the current legal framework. Part II provides an overview of the current legal framework. Part III identifies factors arising from the new technologies and conditions that should be considered when privacy laws are modified to account for the ever-growing capabilities of our surveillance technology.

## I. CHANGING TECHNOLOGIES AND THE CHANGING NATURE OF SURVEILLANCE

The current privacy-in-public standard was developed in the context of unsophisticated visual observation techniques and image-recording equipment with little capability to enhance the abilities of the naked eye. When the current law was developed, a person in a public space could expect to be seen and watched by others, and just as quickly forgotten. The technology and public interest of the time did not encourage the wholesale capture, storage, transmission, and manipulation of visual images, as is common today. Times have changed. The sheer number of cameras monitoring public spaces today makes it difficult to go into public without exposing oneself to continuous and permanent image capture. Few of our actions in public spaces are protected from visual surveillance by current privacy law, either under the search and seizure protections of the Fourth Amendment or the current tort law provisions.

### A. BETTER EQUIPMENT

It is difficult to imagine using pinhole-camera technology in a red-light camera system. Camera technology from just a few years ago would not have provided the image quality necessary for even the most mundane of today's surveillance applications. The ready availability of smaller, better, cheaper cameras and video recorders requires society to address the legal and ethical aspects of capturing and storing images of unwilling or unknowing subjects.

The sophisticated digital surveillance cameras that are now available to the public for very affordable prices[1] have democratized the ability to capture high-quality surveillance images.

[1] Exterior Security Cameras, http://www.123cctv.com (last visited Jan. 2, 2008). Simple analog surveillance cameras are available for less than $50. A mini-dome camera with color, audio, 360 degrees of rotation and an infrared capability that allows images to be captured in almost complete darkness costs under $150. The wireless version costs just a little more. At the high end, an exterior pan, tilt, and zoom (PTZ) camera with a 23x optical zoom and 10x digital zoom (230x overall zoom) that can be controlled by a remote operator is available for less than $1500. *See also* CCTV Online Store, http://www.cctvonlinestore.com/ (last visited Jan. 2, 2008); Security Camera Systems, www.palmvid.com (last visited Jan. 2, 2008); Factory Prices on CCTV Camera Systems, www.cctvfactory.com (last visited Jan. 2, 2008) (examples of the plethora of websites where CCTV equipment can be bought); Extreme

These cameras have amazingly high resolutions, 360° ranges of vision, and incredible zoom and night-vision capabilities.[2] Even more important than the revolution in image capture is the revolution in computing and data-storage technologies. For example, a generation ago, a computer's entire storage capacity was smaller than today's individual files; a few years ago, the storage capacity of an 8GB iPod nano,[3] which can be easily slipped into a pocket and forgotten, was unimaginable; and a few months ago, we could only dream that a TiVO digital video recorder able to store 80 hours of television would be the entry-level model available for less than $100.[4] Increases in computing speed and storage capacities, along with decreases in hardware size, have been critical to the development of surveillance technology. Without these technological advances, cameras and computers would be too big for surveillance purposes, capturing and processing digital images would be too slow to be useful, and the memory needed to store the images digitally would require warehouses full of memory units.

### B. MORE EQUIPMENT

---

Surveillance, www.extremesurveillance.com (last visited Jan. 2, 2008) (information about integrated surveillance systems available to commercial, government, and residential customers).

[2] *See* Exterior Security Cameras, CCTV Online Store, Security Camera Systems, Factory Prices on CCTV Camera Systems, Extreme Surveillance, *supra* note 1.

[3] Apple - iPod nano - Technical Specifications, http://www.apple.com/ipodnano/specs.html (last visited Jan. 2, 2008).

[4] Buy TiVo, https://www3.tivo.com/store/boxdetails.do?boxName=80hourseries2dt&boxsku=R64980 (last visited Jan. 2, 2008).

We are quickly establishing a panopticon[5] in our cities due to the saturation of surveillance cameras.[6] Cameras are everywhere, and many of them are web-enabled. Great Britain is in the lead with approximately 4.2 million Closed-Circuit Television ("CCTV") cameras.[7] In the course of one day, a person in Britain can reasonably expect to be viewed by over 300 cameras.[8] Britain is also integrating its CCTV system with a national Automatic Number Plate Recognition system ("ANPR"),[9] which will be able to read 35 million license plates per day, increasing to 50 million reads per day by 2008.[10]

New York City is doing its best to keep up with Britain, but comes in a distant second with only 10,000 cameras installed.[11] Not everyone in New York is happy about increasing this surveillance. The Institute for Applied Autonomy has published a map of surveillance camera

[5] A famous example of behavior control through surveillance is the Panopticon, which was developed by 18th century philosopher Jeremy Bentham as the ideal, utilitarian prison. Jeremy Bentham, THE PANOPTICON WRITINGS, (Miran Bozovic ed., Verso, 1995) 29-95, *available at* http://cartome.org/panopticon2.htm (last visited Jan. 2, 2008); Observing Surveillance, http://www.observingsurveillance.org/introduction.html (last visited Jan. 2, 2008). (The theory is to arrange the prisoner's cells in a circle around a central guard tower so that the guards can see inside every cell. This allows many prisoners to be monitored by few guards. Window blinds in the guard tower can be adjusted so that the guards can see out, but the prisoners cannot see in. Once the prisoners believe that the guards are watching them, it is not important whether the guards are actually watching or even present; the mere belief that the guards are present is sufficient to keep the prisoners from misbehaving. Thus, observation, or the appearance of observation, is a means of controlling behavior.)

[6] *See* Global CCTV Hub – Blog Toplist, http://www.blogtoplist.com/technology/blogdetails-8105.html (last visited Jan. 2, 2008) (discussion on camera surveillance systems and their use).

[7] SURVEILLANCE STUDIES NETWORK, A REPORT ON THE SURVEILLANCE SOCIETY 19 (David M. Wood ed.,2006), http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf.

[8] *Id.*

[9] *Id.* at 19-20.

[10] *Id.* at 20.

[11] Erin Blakeley & Rodrigo Campos, *Feel Like You're Being Watched? You Are.*, NYC24, http://www.nyc24.org/2006/issue3/story01/index.html (last visited Jan. 2, 2008).

locations so that people can avoid them.[12] The Surveillance Camera Players, a pro-privacy organization, conducts weekend tours of heavily monitored areas of the city, pointing out the cameras.[13] Ironically, these tours have turned the cameras into a tourist attraction, and are listed by Budget Travel Online as a recommended way to see New York.[14]

Public agencies are not the only entities collecting more and more real-time surveillance images; every city in America now has its share of private surveillance cameras that monitor public areas such as sidewalks, parking lots, freeways, and traffic lights. So many of these cameras are integrated with the Internet that any private citizen with a computer and an Internet connection can observe real-time video of people in public places around the world. Our computers have become a window through which we can watch ordinary citizens in such places as Caen, France, as they go about their daily commute,[15] golfers in Hawaii as they start their rounds at the Mauna Lani Resort,[16] weather conditions at the NOAA Amundsen-Scott South Pole Station,[17] or even the activities of penguins in Antarctica.[18] Thousands of web cams in every corner of the world distribute images of street scenes, famous landmarks, and even exhibits

[12] Institute for Applied Autonomy, i-See, http://www.appliedautonomy.com/isee.html (last visited Dec. 20, 2007); New York Surveillance Camera Players, Map of Publicly Installed Surveillance Cameras in New York City, http://www.notbored.org/scp-maps.html (last visited Jan. 2, 2008).

[13] New York Surveillance Camera Players, Surveillance Camera Outdoor Walking Tours, http://www.notbored.org/scowt.html (last visited Jan. 2, 2008).

[14] Blakeley & Campos, *supra* note 11; Budget Travel – Contrarian Tours of Washington, D.C., New Orleans, Houston, and New York City, http://www.budgettravelonline.com/bt-dyn/content/article/2006/02/24/AR2006022401105.html (last visited Jan. 2, 2008).

[15] Caen.maville.com – webcam, http://www.caen.maville.com/vivre/webcam.php?IN_cam=Caen (last visited Jan. 2, 2008).

[16] Mauna Lani Resort Webcams, http://webcam.maunalani.com/webcamgolf.html (last visited Jan. 2, 2008).

[17] ESRL Global Monitoring Division, http://www.cmdl.noaa.gov/obop/spo/livecamera.html (last visited Jan. 2, 2008).

[18] Penguin Webcam – Antarctica, http://www.martingrund.de/pinguine/ (last visited Jan. 2, 2008).

in zoos.[19] Some of the cameras allow the Internet observer to control who, what, and how closely the target subject is observed.[20] Indexes of real-time, or streaming, web cams exist on many websites, so finding real-time video is relatively easy.[21]

Permanently installed surveillance cameras are supplemented by omnipresent cell phone cameras, which collectively create "sousveillance" or a "reverse panopticon" where the watched become the watchers.[22] Cell phone cameras can go where conventional cameras are excluded, for example, at Saddam Hussein's execution,[23] and can provide multiple viewpoints of the same item or event.

### C. The Changing Nature of Surveillance and The Loss of Practical Obscurity

Unlike the beat cop, automated video surveillance sees everything, forgets nothing, and never gets tired or distracted. It captures digital images that can be viewed at any time, from any place, as many times as desired, and can be modified and used well beyond the original intent of

---

[19] Animal Webcams at the National Zoo, http://nationalzoo.si.edu/Animals/WebCams/ (last visited Jan. 2, 2008).

[20] PancakeCam, http://www.pancakecam.com/pancakecam.html; *see generally* EarthCam, http://search.earthcam.com/search/ft_search.php?s1=1&term=interactive+webcam&x=0&y=0, (index of interactive webcams) (last visited Jan. 2, 2008).

[21] Live Webcams, http://www.opentopia.com/hiddencam.php ("These webcams were found automatically through a variety of clever search techniques and update several times a day. Their owners may or may not have intended for them to be public, but they obviously are. Some of them are security cams in companies or semi-public places.") (last visited Jan. 2, 2008); Marcus' Live Streaming Video Cams, http://marcussharpe.com/vidstream.htm (305 streaming cams listed) (last visited Jan. 2, 2008); Web Cams Around the World, www.1000cam.com (" Over 10000 cam from all over the Planet. 290 countries! 100% free viewing!) (last visited Jan. 2, 2008); EarthCam – Webcam Network, http://www.earthcam.com/company/aboutus.php (EarthCam - Where The World Watches The World®") ("EarthCam delivers real time live images of some of the world's most interesting and unique views and events. The portal offers the most extensive database allowing users to search by keyword or simply browse through the categories and subcategories.") (last visited Jan. 2, 2008).

[22] Steve Mann, James Fung & Raymond Lo, *Cyborglogging with Camera Phones: Steps Toward Equiveillance*, http://www.eyetap.org/papers/docs/glogger.pdf (last visited Jan. 2, 2008) ("Sousveillance involves the recording of an activity by a participant in the activity. Usually involves a peer-to-peer approach that decentralizes observation to produce transparency in all directions.").

[23] *More Arrests Expected From Hussein Execution Video*, CNN.COM, Jan. 3, 2007, http://www.cnn.com/2007/WORLD/meast/01/03/saddam.execution/index.html.

either the image collector or the subject. With the extreme zoom capabilities of today's cameras, not only can the camera be so distant from the subject as to make the subject unaware and unsuspecting that surveillance might be present, but the camera can capture a subject's image at a level of intimacy that would be totally unacceptable if the image were observed in person.[24] Not even the cover of darkness provides protection; images can be captured in very low lighting, and can capture information, such as the subject's temperature, that is not apparent to the naked eye.[25]

Even if the beat cop had walked around town with a video camera, the images taken would have enjoyed pseudo-privacy protection through "practical obscurity." The concept of "practical obscurity" applies to public information that is usually outside the public consciousness because it is so difficult to find, like a paper document stored in the dusty basement of the local courthouse[26] or in an infinitely large government warehouse,[27] or by making it difficult to conglomerate large quantities of information. One writer notes:

> [I]n the old days, it took time, talent and tenacity to find out anything. Enter electronic searchability, digital record-keeping and the Internet …. Now even your inquisitive neighbor can ascertain how much you paid for your house, who loaned you the money, your finished square footage and perhaps even your floor plan — without leaving the comfort of his own rather small cottage that he obviously paid too much for. (The reason

[24] Deirdre Mulligan, *Comment*, UnBlinking Symposium, Berkeley, Cal. (Nov. 3–4, 2006).

[25] FLIR Systems, What is Thermal Imaging? What is Infrared?, http://www.corebyindigo.com/applications/irprimer.cfm (last visited Jan. 2, 2008).

[26] U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 764 (1989) (information on a person's rap sheet exists in practical obscurity because its presence in the public record does not make it available for general use); Deveny v. Entropin, Inc. 139 Cal. App. 4th 408, 430 (2006) (in a securities case, information posted on a website about a product's capabilities exists in practical obscurity and cannot be considered public information if the average investor would be unable to locate it without assistance).

[27] Tom Dirks, *Raiders of the Lost Ark (1981)*, GREATEST FILMS, http://www.filmsite.org/raid3.html (last visited Jan. 2, 2008) ("The Ark of the Covenant is crated in a wooden box and its lid is solidly nailed shut. Its stenciled label contains a long inventory number for identification: TOP SECRET, ARMY INTEL 9906753 DO NOT OPEN! A warehouseman pushes the crated Ark down a long aisle formed by huge stacks of similar crates in an enormous government warehouse, where it will again be hidden away - presumably by bureaucratic inefficiency.")

I know this is because I looked it up on the county Web site.)[28]

The concept of practical obscurity applies to surveillance images, as well. Images that once were practically obscure because they were unavailable except as "hardcopies" now exist as digital data files and are stored in easily accessible databases. The posting of surveillance images on the Internet has lifted the veil of obscurity from public information and allowed it to be used in ways that were not anticipated when it was first defined as public. The issue surrounding practical obscurity is not simply whether public information should be public, but more practically, whether public information should always be easy to find and access. In some cases, the public is encouraged to watch and identify individuals or improper behavior.[29] Should such information be openly available on the Internet? Or should some sense of privacy be maintained by making access to the information more deliberate; for example, by requiring a requestor to register online or go to the information's physical storage location?[30]

## II. THE EXISTING LEGAL FRAMEWORK

Under the current laws, a person in a public space has no protection from unwanted video surveillance by either a state or private actor. The legal doctrines that protect persons from unwanted visual surveillance by state or private actors were developed under the basic premise that any person who goes into a public space voluntarily has waived any right to privacy to the

---

[28] Rob Carrigan, *On the Web, 'Practical Obscurity' Has Practically Departed*, NEWSPAPERS & TECHNOLOGY, Jan. 2003, http://www.newsandtech.com/issues/2003/01-03/nt/01-03_carrigan.htm.

[29] *Texas Border Cam Test Catches 10 Illegal Immigrants*, CHICAGO SUN-TIMES, Jan. 8, 2007, at 49; *see also* Texas Border Watch Test Site, http://www.texasborderwatch.com/ (last visited Jan. 2, 2008); *Hundreds Turn In Marijuana Users in Boulder*, SUMMIT DAILY NEWS, Apr. 29, 2006, http://www.summitdaily.com/article/20060429/NEWS/60429001.

[30] *See* Arminda B. Bepko, *Public Availability or Practical Obscurity: The Debate Over Public Access to Court Records on the Internet*, 49 N.Y.L. SCH. L. REV. 967 (2004-05).

extent of his or her person that is visible to passers-by. Given the abilities of the new video surveillance technologies that enhance the naked eye, this basic assumption may no longer be valid.

### A. State Actors: Protections Under The Constitution and Fourth Amendment

The "plain view" doctrine that developed under the Fourth Amendment search and seizure protections provides that state actors do not need a warrant to surveil activities and objects within plain view.[31] No reasonable expectation of privacy exists for persons or activities that can be observed by passers-by with the naked eye or with devices that reasonably resemble the naked eye. This includes situations in which the subject is in a public place,[32] the activity is a matter of public record,[33] or the subject reveals the information voluntarily to other people.[34]

This interpretation is not absolute, however. In *Katz v. United States*,[35] the Supreme Court recognized the right to privacy based on the expectation of the person being observed

---

[31] United States v. Dunn, 480 U.S. 292, 305 (1987) (using a flashlight to see an item otherwise in plain view does not constitute a search); United States v. Barajas-Avalos, 377 F.3d 1040, 1056 (9th Cir. 2004), *cert. denied*, 543 U.S. 1188 (2005) (using a flashlight to look through a window into a darkened structure does not constitute a search); United States v. Lee, 274 U.S. 559, 563 (1927) (using a searchlight to view cases of illegal liquor on the deck of another vessel did not constitute a search).

[32] Rodriguez v. United States, 878 F. Supp. 20, 24 (S.D.N.Y. 1995) (video surveillance by federal agents did not violate the Fourth Amendment because the activity monitored occurred in a public place, specifically a public street where agents were hidden in a van.); McCray v. State, 581 A.2d 45, 48 (Md. 1990) (videotapes of a defendant walking across a public street did not violate the Fourth Amendment because the defendant did not have a reasonable expectation of privacy under these circumstances).

[33] Hatch v. Town of Middletown, 311 F.3d 83, 91 (R.I. 2002) (the release of a child abuse arrest report did not violate the privacy of the subject of the arrest because the report was a public record) (Mr. Hatch was something of a celebrity due to participating in, and eventual winning, the first season of the reality game show *Survivor*).

[34] Willan v. Columbia County, 280 F.3d 1160, 1162 (7th Cir. 2002) (the disclosure of a candidate's past conviction for felony burglary by law-enforcement officers did not violate the candidate's right to privacy because he voluntarily attracted attention to his past by running for public office).

[35] Katz v. United States, 389 U.S. 347, 352-53 (1967) (the subject created a reasonable expectation of privacy for his conversation by going inside a phone booth and closing the door).

instead of the location being observed. Writing for the majority, Justice Stewart noted: "[t]he Fourth Amendment protects people not places."[36] Although *Katz* was a wiretapping case, it is pertinent to visual surveillance because it allows a person under surveillance to demonstrate his or her expectation of privacy by acting in a manner that would preserve privacy in most situations, such as by wearing a hat or facial disguise. Since *Katz* was decided, courts generally recognize that a reasonable expectation of privacy depends upon several conditions: the expectations of the person observed,[37] the behavior or technique used by the observer,[38] and whether one of the persons being observed consented to the surveillance.[39]

The "plain view" doctrine applies even when the passer-by must expend some extra effort to observe the person or activity,[40] such as providing artificial lighting to see objects in the dark.[41] Generally, the more sophisticated and unusual the equipment used by the observer, the less likely the courts will find the surveillance constitutional without a search warrant.[42] For example, using binoculars and other vision-enhancing equipment does not violate the subject's

---

[36] *Id.* at 351.

[37] Bond v. United States, 529 U.S. 334, 338-39 (2000) (a bus passenger may reasonable expect that his baggage will be handled, but it is not reasonable to expect that it will be "felt in an exploratory manner").

[38] United States v. Cuevas-Sanches, 821 F.2d 248, 251 (5th Cir. 1987) (defendant had a reasonable expectation to be free from video surveillance by a camera mounted atop a power pole overlooking defendant's 10-foot-high fence).

[39] United States v. Nerber, 222 F.3d 597, 600 (9th Cir. 2000) (defendants had no reasonable expectation of privacy from secret video surveillance of their hotel room conducted while police informants were present, but did have a legitimate expectation of privacy once police informants had left and they were alone in their hotel room).

[40] Florida v. Riley, 488 U.S. 445, 450-52 (1989) (no warrant needed to observe a backyard greenhouse from a helicopter); Dow Chem. Co v. United States, 476 U.S. 227, 238 (1986) (no warrant needed to photograph an industrial plant from navigable airspace); United States v. Gori, 230 F.3d 44, 52 (2d Cir. 2000) (no warrant needed to look through a door opened to accept a food delivery).

[41] Texas v. Brown, 460 U.S. 730, 739-40 (1983) (plurality opinion) (using a light to see items in a darkened car that were otherwise in plain view did not constitute a search).

[42] Kyllo v. United States, 533 U.S. 27, 34 (2001) (holding that thermal imaging a home's exterior to determine if the temperature was consistent with the growing of marijuana inside the house requires a warrant, because the technology used was not commonplace; privacy could be eroded by advances in police technology).

right to privacy, provided that the observation would be allowed if made without binoculars.[43] Likewise, the subject has a greater expectation of privacy based on the extent and sophistication of the methods he or she uses to protect the activities from prying eyes.[44]

Even though the exterior of a private space is generally considered to be within the public sphere, the courts have considered the nature of the observation technology used when determining whether a warrant is needed.[45] Visual surveillance of the inside of a private space is even allowed without a warrant, although the resident's efforts, or lack thereof, to maintain privacy of the space are relevant.[46]

There is no safety in numbers. If more than one person is observed, a reasonable expectation of privacy is waived by the consent of one of the subjects, even if a warrant for surveillance would otherwise be required and the other persons being observed did not know about the surveillance.[47]

---

[43] United States v. Taborda, 635 F.2d 131, 139 (2d Cir. 1980) (using binoculars to observing the inside of a home is allowed without a warrant if the activities observed are visible from outside without the use of enhancement devices, because the householder has indicated a lack of subjective expectation of privacy by locating the activities where they can be seen from outside).

[44] United States v. Cuevas-Sanchez, 821 F.2d 248, 251 (5th Cir. 1987) (a fence does not guarantee a reasonable expectation of privacy, but it does protect against casual observers); California v. Ciraolo, 476 U.S. 207, 214-15 (1986) (a fence does not establish a reasonable expectation of privacy from observers in the public airways because the backyard was visible to the naked eye of the observers).

[45] *Kyllo*, 533 U.S. at 34 (2001) (holding that thermal imaging a home's exterior to determine if the temperature was consistent with the growing of marijuana inside the house requires a warrant if obtained information that could not otherwise have been obtained without a warrant).

[46] People v. Hicks, 364 N.E.2d 440, 444 (1st Dist Ill. 1977) (failing to draw one's curtains demonstrates a lack of reasonable expectation of privacy); State v. Ward, 617 P.2d 568, 572-73 (Haw. 1980) (failing to draw one's curtains does not necessarily demonstrate a lack of reasonable expectation of privacy in cases where the windows were physically located where no naked-eye observer could see into them); Wheeler v. State, 659 S.W.2d 381, 390 (Tex. Crim. App. 1982), *reh'g granted*, 617 P.2d 381 at 388 (Tex. Crim. App. 1983) (a month-long stake-out to view the inside of a greenhouse through a five-inch gap in exhaust-fan louvers was a sustained and concerted attempt to penetrate the owner's many efforts to ensure the privacy of the greenhouse and violated the owner's reasonable expectation of privacy).

[47] United States v. Nerber, 222 F.3d 597, 604 (9th Cir. 2000).

### B. PRIVATE ACTORS: PROTECTIONS UNDER TORT LAW

When private parties undertake video surveillance of public spaces, neither the Fourth Amendment nor any other provisions of the Constitution are implicated.[48] Many states have a constitutionally guaranteed right to privacy from search and seizure by government actors; fewer states address the issue of privacy in general.[49] For example, New York law addresses secret video surveillance, but only when performed by a law enforcement agency.[50] In Arizona, it is unlawful to videotape persons without their permission, but the law is qualified so that it applies only when the person being observed has a reasonable expectation of privacy and exempts surveillance of private spaces, e.g. department store dressing rooms, when performed for security purposes.[51]

State tort laws provide possible alternative causes of action, including defamation, nuisance, humiliation, trespass, intentional infliction of emotional distress, assault, and breach of contract, as well as infringement of trademark, trade name or copyright, and restitution for unjust enrichment.[52] These laws are not particularly useful unless the surveillance images capture activity that is clearly private, or the images are used in a way that harms the subject or for commercial gain.

---

[48] State v. Diaz, 706 A.2d 264, 265 n.1 (N.J. Super. Ct. App. Div. 1998) (installing a video surveillance system in one's own home found not to implicate the federal or state constitutions because it is done by private individuals and not by the government); Com. v. Kean, 556 A.2d 374, 378 (Pa. Super. Ct. 1989) (breaking into another person's home to install a hidden video cameras did not implicate the federal or state constitutions because it was done by private individuals and not by the government).

[49] Alaska Const. art. I, § 22 (2007); Mont. Const., art. II, § 10 (2005) (examples of state constitutions that have a right to privacy in general).

[50] N.Y. CRIM. PROC. LAW ch. 11-A, pt. 3, tit. T, art. 700 (McKinney 2007).

[51] ARIZ. REV. STAT. ANN. § 13-3019 (2007).

[52] Jeffrey F. Ghent, *Waiver or Loss of Right to Privacy*, 57 A.L.R.3d 16 § 2b.

Surveillors also have rights. A citizen's right to use a video camera in a public place is protected by the Constitution, subject to restriction only by statute.[53] Using a camera is generally a lawful act and taking motion pictures is a reasonable means of securing evidence for trial.[54] Photographing a person in a private place without the subject's consent, however, is not within a citizen's rights, whether or not the photographer actually views the scene at the moment the photograph is taken.[55] Pictures taken in a public space where a person's activities can be observed by passers-by, do not violate a person's right to privacy because the person exposed himself or herself to public observation and therefore was not entitled to the same degree of privacy enjoyed within the confines of one's own home.[56] Photographs taken in a public area of a private facility that is open to all users of the facility do not violate the subject's right to privacy.[57]

### C. Filling The Gaps: Privacy Policies

Public and private organizations have created policies that attempt to fill the voids left by federal and state laws. These organizations have identified the components of an ideal privacy

[53] United States v. Gugel, 119 F. Supp. 897, 898 (E.D. Ky. 1954) ("The operation of a camera is a lawful act and a citizen's privilege to take pictures, unless made specifically unlawful by statute, is such a civil right as is protected by the Constitution of the United States.").

[54] Forster v. Manchester, 189 A.2d 147, 150 (Pa. 1963) (holding that a plaintiff's right to privacy was not invaded when motion pictures were taken of her by a private detective working for the insurer of a driver with whom the plaintiff had been in an automobile accident).

[55] State v. Martin, 658 P.2d 1024, 1027 (Kan. 1983) (secretly photographing young women while they were changing clothes in an attic studio tended to uphold violation of eavesdropping statute which prohibited, inter alia, entering into a private place with intent "to observe the personal conduct of any other person or persons therein").

[56] *Forster*, 189 A.2d at 150.

[57] Muratore v M/S Scotia Prince, 656 F. Supp. 471, 483 (D. Me. 1987), *aff'd in part, and vacated in part*, 845 F.2d 347 (1st Cir. Me.) (photographing a passenger on cruise ship did not state cause of action for invasion of privacy; although photographers harassed passenger on several occasions, the harassment occurred in areas of ship open to all passengers).

policy and have implemented these components in various ways.[58] Examples of national, municipal, and industrial groups, as well as university privacy policies are discussed in this section. Neither the policies nor the organizations included here are comprehensive; these examples are merely a sampling of the variety of privacy policies that have been created by private organizations.

### 1. A NATIONAL POLICY: CCTV CODE OF PRACTICE

In 2000, the Information Commissioner of the United Kingdom issued the CCTV Code of Practice to assist CCTV system operators in understanding their legal obligations, to set out standards that must be followed to ensure compliance with the Data Protection Act 1998, and to reassure the public about safeguards that should be in place.[59] This Code references eight data protection principles, which were promulgated in the Data Protection Act of 1998.[60] These principles state that data must be relevant, not excessive, accurate, and secure; stored only as long as necessary; processed fairly and lawfully; and used for limited purposes in accordance with individuals' rights.[61] In support of these principles, the Code provides that the installation of a CCTV system should be undertaken only in accordance with the following standards:

---

[58] *See generally* THE CONSTITUTION PROJECT, GUIDELINES FOR PUBLIC VIDEO SURVEILLANCE (2007), *available at* http://www.constitutionproject.org/pdf/Video_Surveillance_Guidelines_Report_w_Model_Legislation2.pdf (discussing the relevant issues and containing a section entitled Model Legislation For Establishing Public Video Surveillance Systems).

[59] INFORMATION COMMISSIONER, CCTV CODE OF PRACTICE (2000), *available at* http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/cctv_code_of_practice.pdf. This document is being revised; a consultation draft of the 2007 revisions, entitled CCTV DATA PROTECTION CODE OF PRACTICE: CONSULTATION DRAFT is available at http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/ico_cctv_consultation_draft_final.pdf.

[60] Data Protection Act, 1998, ch. 29 (Eng.), *available at* www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1.

[61] *Id.* at pt. I, § 4.

- The system should fulfill a specific, defined purpose and should be installed only after the need for video cameras is assessed, the person or organization responsible for the operation is identified, and security and disclosure policies are established.[62]
- The location of the cameras, the times of day at which monitoring occurs, and the nature of specific image enhancement technologies used, e.g. infrared cameras, should be carefully considered to ensure that the system is used only as needed to fulfill the system's purpose.[63]
- The quality and resolution of the images should be tailored to the purpose of the monitoring.[64] To help operators determine the level of image quality appropriate for their system, the proposed 2007 revision to the Code identifies four image-quality classifications: (1) sufficient to watch the flow of traffic or movement of a crowd without being able to detect individual figures; (2) sufficient to detect individual figures without being able to see individual faces; (3) sufficient to determine whether or not an individual is recognizable; and (4); sufficient to identify an individual with a degree of certainty that would allow the identification to be used in court. [65]
- The owners of any private spaces that are incidentally included in the captured images should be consulted, and the system operators should be trained to recognize the privacy implications of capturing images of private areas. Signs should be posted to inform the public that the space is being monitored.[66]

---

[62] CCTV CODE OF PRACTICE, *supra* note 59, at 6.

[63] *Id.* at 7, 10.

[64] *Id.* at 9.

[65] CCTV DATA PROTECTION CODE OF PRACTICE: CONSULTATION DRAFT, *supra* note 59, at 8.

[66] CCTV CODE OF PRACTICE, *supra* note 59, at 7.

- A human operator should verify the results of automatic facial recognition processing.[67]
- Images should be retained in a secure location for no longer than necessary, accessible by authorized personnel only in a controlled location, and erased once the defined retention period has expired.[68]
- Requests from third parties to access stored images should be granted only in circumstances that are consistent with the purpose of the system and in accordance with documented disclosure policies.[69] Information concerning each release of stored images should be documented.[70]
- Subjects pictured in the images have a right to access the images in a timely fashion and without being charged an excessive fee.[71] Any person in the image, other than the requester, should be disguised or blurred.[72]

Once the decision has been made to implement a CCTV system, the Code is fairly comprehensive as it pertains to the use of surveillance images, but it presumes a right to collect images of unsuspected persons in public spaces. Encouragingly, the proposed 2007 revision adds a caveat that was missing from the first version:

> CCTV is a privacy intrusive technology capable of putting a lot of law-abiding people under surveillance. You should carefully consider whether to use it; the fact that it is

---

[67] *Id.* at 10.

[68] *Id.* at 11, 12.

[69] *Id.* at 13.

[70] *Id.* at 12.

[71] *Id.* at 15.

[72] *Id.* at 16.

> possible, affordable or has public support should not be the primary motivating factor. You should take into account what benefits can be gained, whether better solutions exist, and what effect it may have on individuals.[73]

### 2. A MUNICIPAL POLICY: THE DISTRICT OF COLUMBIA

The District of Columbia's Metropolitan Police Department ("MPDC") operates a growing system of CCTV cameras,[74] which it alleges is "the most tightly regulated system of its kind in the nation."[75] The system is able to link with other public agency video networks, including those operated by the D.C. Public Schools and the District Department of Transportation. The department denies linking with privately operated camera networks, and states that linking with the photo enforcement cameras it operates would be impossible due to incompatibilities between the different media used by each system.[76]

Highlights of the district's CCTV policies and procedures are posted on the Metropolitan Police Department's website, which also references the municipal code provisions in which the complete regulations are found.[77] According to the information posted on the website, the CCTV system is activated only during major events or emergencies, and only upon authorization

---

[73] CCTV DATA PROTECTION CODE OF PRACTICE: CONSULTATION DRAFT, *supra* note 59, at 6.

[74] Press Release, District of Columbia Metropolitan Police Department, MPD Announces Deployment of Last 19 CCTV Cameras to Help Combat Crime in D.C. Neighborhoods (June 25, 2007), http://newsroom.dc.gov/show.aspx/agency/mpdc/section/2/release/11365/year/2007/month/6. *See also*, Metropolitan Police Department, MPDC's Closed Circuit Television (CCTV) System, http://mpdc.dc.gov/mpdc/cwp/view,a,1238,q,541201,mpdcNav_GID,1545,mpdcNav,|31748|.asp (last visited Jan. 2, 2008). For an evaluation of the system, including photos of the control room, see U.S. GEN. ACCOUNTING OFFICE, VIDEO SURVEILLANCE: INFORMATION ON LAW ENFORCEMENT'S USE OF CLOSED-CIRCUIT TELEVISION TO MONITOR SELECTED FEDERAL PROPERTY IN WASHINGTON, D.C., REP. NO. GAO-03-748 (2003), *available at* http://www.gao.gov/new.items/d03748.pdf.

[75] Metropolitan Police Department, CCTV – Policies and Procedures, http://mpdc.dc.gov/mpdc/cwp/view,A,1238,Q,541586.asp (last visited Jan. 2, 2008).

[76] Metropolitan Police Department, CCTV – Links With Other CCTV Systems, http://mpdc.dc.gov/mpdc/cwp/view,A,1238,Q,541579.asp (last visited Jan. 2, 2008).

[77] CCTV – Policies and Procedures, *supra* note 75.

of the Chief of Police or his designee.[78] All CCTV activities must be monitored by an MPDC official with the rank of lieutenant or above; under elevated threat levels, supervision will be assumed by an assistant chief.[79] Camera operators must certify that they understand the policies and procedures, and must not target or track individuals based on a classification that is legally protected.[80] Only public locations where there is "no reasonable expectation of privacy"[81] are targeted and areas monitored by permanent cameras are posted.[82] Cameras will not focus on printed materials, such as handbills or flyers, distributed or carried pursuant to the First Amendment.[83] Video images are recorded only with proper authorization and are deleted after ten days unless needed for potential litigation.[84]

### 3. AN INDUSTRY POLICY: IBM PRIVACY FACTORS

Researchers at the IBM T.J. Watson Research Center have identified six factors that should be addressed in a privacy policy.[85] Like the CCTV Code, the IBM factors provide that the data collected should be limited to that which is necessary to complete the task,[86] accessible

---

[78] *Id.*

[79] *Id.*

[80] *Id.*

[81] *Id.*

[82] *Id.*

[83] *Id.*

[84] *Id.*

[85] Andrew Senior et al., *Blinking Surveillance: Enabling Video Privacy through Computer Vision*, IEEE SECURITY & PRIVACY, May/June 2005, at 50.

[86] *Id.* at 52.

only to authorized personnel,[87] and stored no longer than necessary in order to limit the nature and extent of the data usage.[88] The IBM factors differ from the CCTV Code in a few areas. First, IBM feels that the subjects' consent should be obtained.[89] If that is not possible, then signs should be posted to inform people using the space that it is under surveillance.[90] Second, the stored data should be encrypted, or otherwise appropriately protected from misuse.[91] Third, authorization levels should distinguish between different needs for data access; for example, an "ordinary user" would have access to statistical information about the video, a "privileged user" would have access to limited individual information, and only law enforcement personnel would have access to the raw video and unlimited individual identity information.[92] As part of this discussion, the IBM researchers identified three levels of surveillance anonymity.[93] The first level preserves the most anonymity of the subjects, and is found in garden-variety CCTV systems that do not use zoom lenses or computer enhancement techniques.[94] The second level provides relative identification of the subjects. These systems recognize subjects for short periods of time, but they have no individual information about the subjects.[95] The third level, with the least anonymity, is provided by systems having the capability for absolute identification

[87] *Id.*

[88] *Id.* at 53.

[89] *Id.*

[90] *Id.*

[91] *Id.*

[92] *Id.* at 54.

[93] *Id.* at 52.

[94] *Id.*

[95] *Id.*

based on face-recognition or electronic ID swipes.[96] Third-level systems require that the subjects enroll in the system, and can associate the subject with a database record of personal information.

Finally, consideration should be given to what enhancements should be stored with the video images, and whether privacy-invasive features should be masked.[97]

### 4. A UNIVERSITY POLICY: THE UNIVERSITY OF PENNSYLVANIA

The University of Pennsylvania Department of Public Safety has promulgated a video surveillance privacy policy that incorporates most of the factors addressed by IBM and the CCTV Code, and provides further standards regarding oversight and training.[98] The policy specifies the responsibilities of everyone involved in CCTV operations, and identifies the parties responsible for overseeing the daily operation of the system, keeping current with any changes in relevant law and security industry practices, and authorizing all CCTV monitoring.[99]

The policy establishes a CCTV Monitoring Panel to review the camera locations, requests for data access, and the policy itself; and to ensure that the group directly in charge of the program adheres to established policy and procedure.[100] The faculty, staff, students, university president, and the Safety and Security Committee are each represented on the panel.[101]

---

[96] *Id.*

[97] *Id.*

[98] UNIVERSITY OF PENNSYLVANIA, CLOSED CIRCUIT TELEVISION MONITORING AND RECORDING OF PUBLIC AREAS FOR SAFETY AND SECURITY PURPOSES, *available at* http://www.publicsafety.upenn.edu/downloads/Policy_CCTV_Monitoring_and_Recording.pdf (last visited Jan. 2, 2008).

[99] *Id.*

[100] *Id.*

[101] *Id.*

Any member of the panel may audit monitoring operations, including videotape storage, at any time without prior notice.[102] The policy defines the procedure by which decisions by the panel can be appealed, including how to file a petition to forgo installation of a proposed camera or to request the removal of an existing camera.[103]

Personnel involved in video monitoring must be appropriately trained and continuously supervised.[104] Training must include technical, legal, and ethical parameters of appropriate camera use, as well as cultural awareness.[105] Operators must receive, understand, and acknowledge the CCTV policy.[106]

Data collection may be authorized for legitimate safety and security purposes only.[107] Collecting data for any purpose other than deterring crime and promoting campus safety is prohibited.[108] Data collection is limited to what is visible with unaided vision.[109] Surveillance of residential lounges and hallways is strictly forbidden unless the Vice President of Public Safety determines that a specific risk exists.[110] The surveillance system will not target people becoming intimate in public areas, look through windows to view private rooms or areas, nor target individuals based on race, gender, ethnicity, sexual orientation, disability, or any other

---

[102] *Id.*

[103] *Id.*

[104] *Id.*

[105] *Id.*

[106] *Id.*

[107] *Id.*

[108] *Id.*

[109] *Id.*

[110] *Id.*

classification protected by the University's non-discrimination policy.[111] Information gained in violation of the procedures will not be used in any disciplinary proceeding against faculty, staff, or students.[112]

The video surveillance policy and guidelines, and the locations and capabilities of CCTV cameras are published semi-annually in the campus newspaper and can be requested at any time.[113] The locations being monitored are appropriately signed.[114] The locations of temporary cameras for special events will be published before the event, if possible.[115]

CCTV monitoring centers must be configured to prevent tampering with or duplicating recorded information.[116] Information is to be used exclusively for security and law enforcement purposes, and will be released only when authorized by the Vice President of Public Safety according to procedures established in the policy.[117] Videotapes are to be stored in a secure location accessible to authorized personnel only.[118] The release of videotapes requires the approval of the Monitoring Panel and the Vice President of Public Safety, except for videotapes directly related to criminal investigations.[119] Release will be approved only for legitimate purposes and requires at least five affirmative votes.[120]

---

[111] *Id.*

[112] *Id.*

[113] *Id.*

[114] *Id.*

[115] *Id.*

[116] *Id.*

[117] *Id.*

[118] *Id.*

[119] *Id.*

[120] *Id.*

## III SURVEILLING THE FUTURE

Changes in video surveillance technologies, the amount of video surveillance images being captured in public spaces, and society's changing attitudes towards surveillance require us to reevaluate the factors used to measure the right to privacy from public video surveillance. The subject's ability to see the video surveillance camera, to anticipate the type of images being captured, to know who, how, where, and when the images will be used, and to control the use of personally identifiable information are important factors that should be considered. These factors inform fundamental questions concerning the right to know that one is under video surveillance, the existence of meaningful choices about participating in video surveillance, and the ability to control one's image data.

### A. DISTANCE AND MAGNIFICATION

Privacy laws should consider the distance between the surveillance camera and the subject, and the level of magnification used. The distance between the camera and the subject is an important factor because the reach of today's technology allows surveillance systems to capture images of persons who are unaware of being observed. Although the images captured are similar to what would be seen by a passer-by, the subject is not aware of the surveillance, and thus cannot choose to leave the area being surveilled or otherwise indicate an unwillingness to participate in the surveillance. Magnification allows the observer to see the subject, or parts of the subject, at a level of detail that is not normally visible to others. Unlike the distance issue, a passer-by in this case would not be able to see the same view as the video surveillance system unless the passer-by was permitted to be in intimate proximity to the subject. Again, the subject

of the surveillance cannot rely on seeing the camera, the size of the lens, or the location of the person capturing the subject's image, to adequately judge the type of image being captured and respond appropriately.

### B. IMAGE DURABILITY AND DISTRIBUTION

Privacy laws should consider how long a video surveillance image is kept and whether it is available to viewers far distant from the place where the image was captured. Unlike the beat cop, video surveillance images can be watched long after they were captured and far removed from the place they were captured. The subject of the image capture has no way to know how far away in time and space his or her images will be seen and thus has no way to judge whether to opt-out of participating.

### C. SELECTING AND TRACKING THE SUBJECT

Privacy laws should consider the video surveillance system's ability to select and track individual subjects. Surveillance began as a means to track "shady characters" that were suspected of some wrongdoing. Slowly this changed, first as society installed video surveillance cameras at places with a high potential for criminal activity, such as ATMs, banks, and gas stations, and then as surveillance cameras began watching people who were not suspected of any wrongdoing and were not in places prone to crime. As the use of cameras that are controlled by human operators increases, the chance that operators will use their power inappropriately,[121] or that protected classes of people will be singled out for surveillance also increases.

[121] Abuses of Surveillance Cameras, http://www.notbored.org/camera-abuses.html (last visited Jan. 2, 2008) (listing multiple instances of casino surveillance camera operators who turned the cameras into a "peep show" by targeting specific body parts of female gamblers and employees, and police officers who misused surveillance cameras, among others).

> During my time in the control room, from 9 p.m. to midnight, I experienced firsthand a phenomenon that critics of CCTV surveillance have often described: when you put a group of bored, unsupervised men in front of live video screens and allow them to zoom in on whatever happens to catch their eyes, they tend to spend a fair amount of time leering at women…. In Hull, this temptation is magnified by the fact that part of the operators' job is to keep an eye on prostitutes. As it got late, though, there weren't enough prostitutes to keep us entertained, so we kept ourselves awake by scanning the streets in search of the purely consensual activities of boyfriends and girlfriends making out in cars…. [O]perators, in addition to focusing on attractive young women, tend to focus on young men, especially those with dark skin.[122]

### D. UNAUTHORIZED IMAGE USE AND MODIFICATION

Privacy laws should consider the nature and extent of any unauthorized use or modification of the captured image. The privacy implications of the misuse of human images was one of the frontiers boldly explored by Gene Roddenberry and the creators of the TV series "Star Trek: The Next Generation" ("TNG"). Two episodes of TNG specifically addressed the use and abuse of human images.[123]

In "Hollow Pursuits,"[124] Ensign Barclay creates holographic versions of the senior officers and uses them to play out his fantasies on the holodeck. In TNG, the holographic images are so lifelike that they are physically indistinguishable from the real people, but Barclay modifies the holograms so they are subservient to Barclay, totally unlike their real counterparts. When the senior officers find out about Barclay's activities they feel violated, both by the mere existence of the images and by the way their holographic selves have acted. One officer comments that although there is no rule against what Barclay did, "there should be."

---

[122] Jeffrey Rosen, *A Watchful State*, N.Y. TIMES, Oct. 7, 2001, *available at* http://www.nytimes.com/2001/10/07/magazine/07SURVEILLANCE.html.

[123] Paul Joseph & Sharon Carton, *The Law of the Federation: Images of Law, Lawyers, and the Legal System in "Star Trek: The Next Generation"*, 24 U. TOL. L. REV. 43, 80-83, 1992.

[124] StarTrek.com, Episode, http://www.startrek.com/startrek/view/series/TNG/episode/68444.html (last visited Jan. 2, 2008).

In "Booby Trap,"[125] Geordi La Forge, the chief engineer, creates a holographic representation of Leah Brahms, the woman who designed the ship's engines, to obtain assistance during an engineering emergency. Unlike Ens. Barclay's creations in "Hollow Pursuits," the holographic image of Leah Brahms is extremely realistic because La Forge based it on her personnel file.[126] While working together on the engineering emergency, La Forge develops a personal relationship with the holographic Leah Brahms. When the real Leah Brahms comes aboard in a later episode,[127] La Forge treats her in a manner consistent with a prior relationship. Understandably, she finds his behavior overly familiar and entirely inappropriate; for her, this is their first meeting, for La Forge, however, they are close friends. When the real Leah Brahms finds out about the holographic Leah Brahms, she also feels violated by the way "she" has been used.

The Star Trek writers recognized that people want to control their images, regardless of whether the image is an accurate reflection of them or is modified to meet the possessor's needs. Although the technology used in TNG to use and misuse images is beyond our reach, the desire to "enhance" the images of others goes back as long as there have been images on which to draw mustaches.

---

[125] StarTrek.com, Episode, http://www.startrek.com/startrek/view/series/TNG/episode/68414.html (last visited Jan. 2, 2008).

[126] A discussion of the Federation's privacy laws and whether an engineering emergency is a valid reason for violating them will have to wait for another Note. Further enlightenment about Federation law in general is available at Joseph & Sharon, *supra* note 120.

[127] StarTrek.com, Episode, http://www.startrek.com/startrek/view/series/TNG/episode/68486.html (last visited Jan. 2, 2008).

In real life, the misuse of visual images is also a concern. Spencer Tunick is famous for photographing urban landscapes containing large numbers of nude people.[128] In March 2006, Tunick photographed approximately 1700 people in Newcastle, England. The photos were taken in an urban area populated with private surveillance cameras, many of which captured images of participants as they walked naked from the staging area to the location where the photograph was taken. It was discovered afterwards that the camera operators, including police department employees, had obtained stills of the nude people from the surveillance camera video and offered them for sale at the local bars and pubs, even at the subjects' own locals.[129] The police department promised to investigate.[130]

Within this situation lies a deeper question of how to allocate the risk that video surveillance images will be misused. Since the person with possession of the video surveillance images is the only one who will know for certain whether the images exist, surely the possessor is in the best position to bear the burden of safeguarding the images.

### E. VIDEO IMAGES ARE PERSONALLY IDENTIFIABLE INFORMATION

[128] See examples of his work at I-20 Gallery: Selected Images of Spencer Tunick, http://www.i-20.com/artist.php?artist_id=19 (last visited Jan. 2, 2008).

[129] Hille Koskela, (Re)exposing the Naked Body: The Misuse of Surveillance Cameras in Spencer Tunick's Photography Event, UnBlinking: Symposium, Nov. 3–4, 2006, http://www.law.berkeley.edu/institutes/bclt/events/unblinking/unblinking/koskela-unblinking-abstract.htm (last visited Jan. 2, 2008); Oliver Duff, *Film of Artist's Mass Nude Photo Shoot Being Sold in Pubs*, THE INDEP. ONLINE EDITION, Mar. 21, 2006, http://news.independent.co.uk/uk/this_britain/article352607.ece.

[130] Duff, *supra* note 126.

Video surveillance images are data and may contain personally identifiable information ("PII").[131] Therefore, these images should be subject to the same protections as other forms of personally identifiable information.

Like fingerprints and retina patterns, facial images captured by video surveillance systems are biometric information that can be used to uniquely identify individuals.[132] Facial images, when combined with location, place, and time information provided by the capturing surveillance camera, uniquely identify a person at a specific place and time. Face recognition technology allows absolute and relative identification of subjects. Absolute identification matches a face to a name; relative identification matches a face to a face. Face recognition technology searches through images to find all occurrences of a "tagged" facial image.[133] This can be used to find occurrences of the same face in situations where a name is provided, which could be devastating to the privacy of individuals whose facial images are captured at political rallies or abortion clinics. Even if the surveillance images are de-identified by randomly altering certain data fields, such as date and time, so that the information is no longer PII, it is possible to

[131] PII is information that "identifies or can be used to identify, contact, or locate the person to whom such information pertains. This includes information that is used in a way that is personally identifiable, including linking it with identifiable information from other sources, or from which other personally identifiable information can easily be derived, including, but not limited to, name, address, phone number, fax number, email address, financial profiles, social security number, and credit card information. To the extent unique information (which by itself is not Personally Identifiable Information) such as a personal profile, unique identifier, biometric information, and IP address is associated with Personally Identifiable Information, then such unique information will also be considered Personally Identifiable Information…." Privacy Definitions, http://www.p3pwriter.com/LRN_000.asp#PII (last visited Jan. 2, 2008).

[132] Electronic Frontier Foundation, Biometrics: Who's Watching You (Sept. 2003), http://www.eff.org/wp/biometrics-whos-watching-you.

[133] Riya – Visual Search, http://www.riya.com/ (last visited Jan. 2, 2008) ("Find an item you like, and Like.com will show you items that are visually similar.") (supports searches for objects and people). *See also* Eigenfaces/Photobook Demo, http://vismod.media.mit.edu/vismod/demos/facerec/basic.html (last visited Jan. 2, 2008); Jacqui Cheng, *Facial Recognition Slipped Into Google Image Search*, ARS TECHNICA, May 30, 2007, http://arstechnica.com/news.ars/post/20070530-facial-recognition-slipped-into-google-image-search.html ("While currently unofficial and unannounced, users can now search for images that only contain faces by appending a query string onto the end of a search URL.").

re-identify the information if there are enough distinct pieces of de-identified data available or simply through clever technology.[134]

Under the current law, the right to distribute images of a subject belongs to the person who captured the images and not the subject. However, if the images are PII, then current privacy law supports the idea that the person whose data is captured, i.e. the subject of the surveillance, retains the right to control that data. In addition, other rules that apply to personal information, such as the Fair Information Practices Act of 1973,[135] would apply to facial images captured by video surveillance systems. An Internet-enabled video surveillance system that captures images of children might also by subject to the parental permission restrictions of the Children's Online Privacy Protection Act ("COPPA").

### F. CORRELATING DATA FROM MULTIPLE SOURCES

Privacy laws should consider whether the surveillance image could be combined with information of other types or from different sources. For example, the District of Columbia Police Department has the ability to link its CCTV network with other public agency video networks, such as the traffic cameras operated by the Department of Transportation and the

---

[134] *Interpol: Pedophile in Photo ID'd as Teacher*, MSNBC.COM, Oct. 16, 2007, http://www.msnbc.msn.com/id/21307230/.

[135] The Fair Information Practices Act of 1973 outlines basic principles of data usage:

> **1.** There must be no personal data record-keeping systems whose very existence is secret;
> **2.** There must be a way for an individual to find out what information is in his or her file and how the information is being used;
> **3.** There must be a way for an individual to correct information in his or her records;
> **4.** Any organization creating, maintaining, using, or disseminating records of personally identifiable information must assure the reliability of the data for its intended use and must take precautions to prevent misuse; and
> **5.** There must be a way for an individual to prevent personal information obtained for one purpose from being used for another purpose without his or her consent.

CDT's Guide to Online Privacy, Privacy Basics: HEW Code of Fair Information Practices, http://www.cdt.org/privacy/guide/basic/hew.html (last visited Jan. 2, 2008).

CCTV network operated by the DC Public Schools.[136] Likewise, the British CCTV system recently added loudspeakers to its system to create "speaker cams" that can scold persons observed engaging in "anti-social behavior," such as littering.[137] New York City plans to network thousands of private and public video surveillance cameras, electronic license plate readers, and remote-controlled traffic barriers, controlled by a 24-hour command center.[138]

The same technological advances that make sophisticated surveillance systems possible also allow the collection of vast quantities of personal data, including credit card purchases, EZ Pass usage, car registration information, grocery store loyalty programs, library borrowing records, and any other records that are kept digitally.[139] "Dataveillance" is the term coined to describe the practice of automatically correlating one person's information from multiple sources.[140] For example, credit card gas purchases could be compared with purchases from auto service centers to estimate the number of miles driven since the last servicing. Based on this, a reminder that servicing is needed could be sent to the vehicle owner. The same technique could be used to compare car registration information with insurance company records so that drivers without insurance could be flagged. Dataveillance by government entities has been called "the technological equivalent of a general warrant on the entire population," because everyone is presumed guilty until proven innocent.[141] It violates the privacy principle that personal

---

[136] CCTV – LINKS WITH OTHER CCTV SYSTEMS, *supra* note 73.

[137] Will Byrne, *Orwell Rolls in His Grave: Britain's Endemic Surveillance Cameras Talk Back*, RAW STORY, May 30, 2007, http://rawstory.com/printstory.php?story=6292.

[138] Alex Kingsbury, *Gotham's Sky Spies*, U.S. NEWS & WORLD REPORT, July 23, 2007, *available at* http://www.usnews.com/usnews/news/articles/070715/23cctv.htm.

[139] Posting of Bruce Schneier to Schneier on Security: The Future of Privacy (Mar. 6, 2006), http://www.schneier.com/blog/archives/2006/03/the_future_of_p.html.

[140] AUSTRALIAN PRIVACY FOUNDATION, AUSTRALIA AS A SURVEILLANCE SOCIETY (Jun. 30, 1994), http://www.privacy.org.au/Papers/SubmnNSWParlt9406.html.

[141] *Id.*

information supplied for one purpose should not be used for another purpose without express consent from the individual concerned.[142]

The possibilities presented by dataveillance explode when data is combined with visual images. With dataveillance, the identity of the person or vehicle often must be inferred from usage of a credit card. Surveillance videos capture uniquely identifying information, such as faces and license plates. With a license plate tracking system like the one being installed in Great Britain, it is possible to know not only how many miles were traveled, but also where the vehicle went. If a data collection and control system like GM's OnStar[143] were combined with information from municipal traffic light cameras, then it would be possible to create a system where the driver of a vehicle caught running red lights could be scolded by the OnStar operator and the car deactivated. In this scenario, Big Brother becomes "Mom cam."[144]

It is easy to imagine a time, not so far from now, when we will have the technology to aggregate surveillance cameras, biometric identification systems, and other discrete monitoring systems into a vast network of real-time surveillance. It will allow us to locate particular individuals anywhere at anytime, to know where they have been, where they are going, who they are with, who they are likely to meet, and even what the person has with them. Omniscient, omnipresent visual surveillance will certainly not be "the end of western civilization as we know it," but it will change the way we act. The question is not whether we will react, but what the nature and extent of the reaction will be, and what will be lost in the inevitable cat-and-mouse game between the observers and the observed.

---

[142] *Id.*

[143] OnStar By GM, http://www.onstar.com (last visited Jan. 2, 2008).

[144] *See e.g.*, *Stop Thief! GM's OnStar Could Stop Stolen Cars*, MSNBC.COM, http://www.msnbc.msn.com/id/21134540/vp/21206876#21206876 (last visited Jan. 2, 2008).

## CONCLUSION

Privacy is not a static, one-size-fits-all concept. New surveillance technologies and changing societal views towards information sharing constantly change the calculus of privacy law. The calculus becomes more complex because new technologies and changing societal norms may work toward opposite ends; new technologies make video surveillance more intrusive and suggest the need to strengthen privacy laws, while changes in societal norms indicate more acceptance of sharing one's personal information and suggest that expectations of privacy are becoming weaker. Regardless of the net direction of these changes, it is clear that factors that were appropriate when the beat cop was responsible for the surveillance of public spaces need to be reconsidered in light of new technologies used in the video surveillance of public spaces.