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

_____
Katie Black
IPIOP Clerk

_____
Meghan Murtha
IPIOP Clerk

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

Filed: January 15, 2008