PAN, TILT, ZOOM: REGULATING THE USE OF VIDEO SURVEILLANCE OF PUBLIC PLACES

By Jeremy Brown

I. INTRODUCTION

Local governments have been using video cameras to surveil public areas for four decades. In that time, legislatures and courts have generally refrained from regulating such use. In recent years, though video surveillance systems have begun to change. Gone are the days of stand-alone cameras that record grainy images onto bulky tapes. In their place are integrated camera networks equipped with intelligent software and almost limitless storage capacity. Facial recognition programs and tracking mechanisms are in the works. Such developments in video-surveillance technology could help police combat crime. But they could also erode privacy rights and substantially change the character of public places.

This Note argues that the government should regulate police use of video systems to surveil public areas. This regulation could take many forms but would, at its core, answer two key questions: 1) how should police use video surveillance; and 2) for what purpose should they use it? All levels of government could enact laws that would help to answer these questions, but regulation cannot succeed without action from local governments. It is the officials in police stations and city hall chambers who know most about their individual systems and are in positions to create rules that can efficiently govern their day-to-day operations. Many of those same officials have so far failed to create rules, however. The federal government and state governments could step in and encourage local governments to create operational rules. At the same time, they could develop laws that are grounded in their particular areas of authority and expertise.

Part II reviews the history of municipal use of video surveillance systems in the United States. It argues that while technological limitations prevented police from misusing surveillance systems in the past, a new generation of video systems is more susceptible to misuse because it does not face these limitations. Regulation, if properly crafted, could help to prevent misuse.

Part III explores the inadequacy of judicial regulation. Courts have recognized some limits on the use of video surveillance. But those lim-

its—many of which are found in the dicta of cases addressing other forms of surveillance—are hazily defined and largely untested. The systems in use and in development are not technologically advanced enough to bump against those limits. As a result, lower courts may not have the means to soundly and effectively regulate video surveillance until the Supreme Court creates a new framework for assessing Fourth Amendment privacy rights.

Part IV discusses federal regulation, arguing that Congress should pass video surveillance legislation and that the E-Government Act of 2002 could offer a model.[1] States should also consider regulatory legislation. The states are uniquely positioned to address some of the issues that video surveillance raises and, in the absence of federal action, could help to fill the regulatory gap.

Part V argues that local governments must regulate their video systems. They can do so—at an operational level—by developing policies and procedures similar to those that govern many other police practices.[2] Such policies could complement state and federal legislation and could provide numerous benefits for local governments.

Part VI concludes that regulation is not enough. In the area of video surveillance, where police have significant discretion and limited oversight, custom is as important as law. If regulation is to succeed, police must create and promote best practices that respect the spirit of that regulation.

II. MUNICIPAL USE OF VIDEO SURVEILLANCE

A. Evolution of Video Surveillance

Local law-enforcement agencies did not adopt surveillance cameras until the late 1960s because of concerns about "underdeveloped technology, excessive cost and unfavorable public opinion."[3] In 1971, the city of

1. Pub. L. No. 107-347, 116 Stat. 2899. The Act requires federal agencies to conduct privacy impact assessments before "developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form." 44 U.S.C. § 3501 (Supp. II 2002).

2. *See, e.g.*, MADISON POLICE DEP'T., CITY OF MADISON, MADISON POLICE POLICY MANUAL, *available at* http://www.ci.madison.wi.us/POLICE/PDF_Files/PolicyandProcedureManual.pdf (describing procedures for videotaping demonstrations, in-car video capture, and storing video evidence); CITY OF BALTIMORE, CITIWATCH AT THE ATRIUM POLICIES AND PROCEDURE MANUAL (2008) (describing procedures for network of hundreds of all-weather fixed surveillance cameras).

3. Robert R. Belair & Charles D. Bock, *Police Use of Remote Camera Systems for Surveillance of Public Streets*, 4 COLUM. HUM. RTS. L. REV. 143, 147 (1972).

Mt. Vernon, New York, unveiled a federally funded two-camera system that the Department of Justice considered a prototype for future surveillance systems.[4] The DOJ installed two cameras one block apart and mounted them atop utility poles.[5] Officers used and controlled the cameras remotely from the police station.[6] The cameras could rotate 355 degrees horizontally and tilt up to 120 degrees vertically, allowing them to peer through the windows of ground-floor shops.[7] Still, the state-of-the-art system had limitations.[8] Among them was the cost of tapes, which were so expensive that police departments had no choice but to regularly record over them.[9]

Cameras have come a long way in the decades since the Mt. Vernon experiment.[10] They can now be linked to form integrated systems that cover not just a few downtown blocks but large stretches of public space.[11] Extensive digital networks can support the transmission of video signals and provide data to police officers who are in the field.[12] Cameras can cap-

---

4. *Id.* at 143-44. The Mt. Vernon system attracted considerable press attention. Publications such as *Time Magazine, T.V. Guide*, the *Chicago Tribune*, and the *Cleveland Press* featured articles about it. John Glenn, the astronaut and soon-to-be Ohio senator, narrated a network documentary in which Mt. Vernon police described zooming in through a restaurant window and viewing a pristine close-up of a diner's sandwich. *Id.* at 145.

5. *Id.* at 144.

6. *Id.* at 144-45.

7. *Id.* at 145 n.14.

8. *Id.* at 144-45.

9. *Id.* at 145.

10. This Note focuses on the public-sector use of cameras. Private actors, however, have also begun to use cameras in ways that could erode expectations of privacy. *See, e.g.*, Aimee Jodoi Lum, Comment, *Don't Smile, Your Image Has Just Been Recorded on a Camera-Phone: The Need for Privacy in the Public Sphere*, 27 U. HAW. L. REV. 377 (2005).

11. CONSTITUTION PROJECT, GUIDELINES FOR PUBLIC VIDEO SURVEILLANCE: A GUIDE TO PROTECTING COMMUNITIES AND PRESERVING CIVIL LIBERTIES xi (2007), *available at* http:// www.constitutionproject.org/pdf/Video_surveillance_guidelines.pdf.

12. Mesh networks offer particular promise. Traditional wireless hotspots restricted access to relatively confined geographical areas. But mesh networks—networks in which many wireless signals link together to form a blanket of coverage—have further reach. A Motorola mesh network, for instance, has girded the Los Angeles Police Department's video surveillance network at the notoriously crime-plagued Jordan Downs housing project. Mark Lacter, *Motorola's High-Speed Wireless Networks Give Cops Slick New Tools to Fight Crime*, WIRED, Nov. 2007, at 54. Some developers of mesh network technology have said that public sector need for security wireless systems has fueled the domestic demand for their products. *See* Press Release, Firetide, Inc., Firetide Ablaze with Eight Consecutive Quarters of Record Revenue Growth (Oct. 23, 2007), *available at* http:// www.firetide.com/ innercontent.aspx?taxid=16&id=892; Rosie Lombardi, *Wi-Fi Growth*

ture images at high resolutions and can be equipped with infrared vision and motion detection technologies.[13] Users can program cameras to automatically track, archive, and identify "suspect behavior."[14] The technology continues to push ahead: the U.S. Department of Homeland Security (DHS) is testing a program that would allow its agents to use cell phones and e-mail devices to record and share live video footage of suspected terrorists, and the French Interior Ministry has announced it would begin using flying drones outfitted with night-vision cameras to monitor crime.[15]

Concerns about crime and terrorism have increased the appeal of surveillance cameras.[16] Camera enthusiasts and critics alike have pointed to the camera system in Britain—home to about a fifth of the world's surveillance cameras[17]—as a harbinger of what video surveillance may eventually be like in the United States.[18] In Britain, there are at least 4.2 million cameras, or one for every fourteen residents.[19] In London, the average person is caught on camera 300 times a day.[20]

The most advanced American video surveillance network is in Chicago.[21] The city has linked together cameras from the transit and housing

---

Fuels Video Surveillance, NETWORK WORLD, Oct. 29, 2007, http://www.networkworld.com/news/2007/102907-wi-fi-growth-fuels-video-surveillance.html.

13. CONSTITUTION PROJECT, *supra* note 11, at xi.

14. *Id.*

15. Mimi Hall, *Surveillance System Raises Privacy Concerns*, SCI-TECH TODAY, Mar. 3, 2008, http://www.sci-tech-today.com/story.xhtml?story_id=0100010W171S; *France to Strengthen Video Surveillance System*, REUTERS, Oct. 12 2007, http://www.reuters.com/article/technologyNews/idUSL1272534220071012.

16. The global market for "network video surveillance products" increased more than 40% in 2006 and is expected to reach $2.6 billion in sales by 2010. Press Release, IMS Research, Network Video Surveillance Market Surges Ahead (Jan. 23, 2007), *available at* http://www.imsresearch.com/members/pr.asp?X=329. Public sector demand is fueling much of that growth. Lombardi, *supra* note 12.

17. Libby Brooks, *CCTV is No Silver Bullet—It Risks Making Life Less Safe*, GUARDIAN, Nov. 1, 2007, at 34.

18. *See, e.g.*, Dina Temple-Raston, *In U.S., Calls Grow for U.K.-Style Security Cameras*, NAT'L PUB. RADIO, July 4, 2007, http://www.npr.org/templates/story/story.php?storyId=11737314; Steve Chapman, *Video Cameras, Safety and Our 'Personal Space,'* CHI. TRIB. July 28, 2005, at C23. American cities have also taken cues from casinos. *See* Thomas Frank, *Face-Recognition Systems Weighed as Next Weapon Against Terrorism*, USA TODAY, May 10, 2007, at 1A; Marie Woolf, *ID Cards Could Be Used for Mass Surveillance System*, INDEPENDENT, Aug. 18, 2005, at 15; Vicki Haddock, *Hundreds of Thousands of Surveillance Cameras Across America Track Our Behavior Every Day*, S.F. CHRON., Oct. 17, 2007, at E1.

19. Brooks, *supra* note 17, at 34.

20. *Id.*

21. Don Babwin, *Chicago Video Surveillance Gets Smarter*, ABC NEWS, Sept. 27, 2007, http://abcnews.go.com/print?id=3659139 (quoting an IBM video surveillance con-

authorities and other governmental agencies.[22] The city hired IBM to install analytic software that would potentially allow network operators to program the cameras to automatically recognize the colors, makes, and models of cars.[23] The cameras would also alert the police of specific events, such as if a car has circled the Sears Tower, or if someone has left a bag unattended in a crowded park.[24]

Cities of all sizes have adopted video systems. A 2006 study found that at least thirty-six California cities—such as Beverly Hills, Stockton, and San Francisco—have installed cameras.[25] So many cities across the country have installed or upgraded systems that research analysts estimate that the video surveillance market will almost double between 2006 and 2011, growing from $6.6 billion to $11.9 billion.[26] The head of the Los Angeles Police Department's Counter-Terrorism and Criminal Intelligence Bureau estimates that the number of police cameras in L.A. could expand tenfold.[27] Such robust prospects have drawn large technology companies into competition with traditional physical security companies[28] and have inspired a few high schools to offer occupational classes in security design.[29]

B. No Regulation of Video Surveillance of Public Places

A public place is generally considered to be one in which individuals do not have reasonable expectations of privacy.[30] The result is that, "according to the law, everything that occurs in a public place cannot be held

---

sultant as saying that "Chicago is really light years ahead of any metropolitan area in the U.S. now").

22. Gary Washburn, *Camera Network to Watch Over City*, CHI. TRIB., Sept. 10, 2004, at C1.

23. David Schaper, *Chicago's Video Surveillance Gets Smarter*, NAT'L PUB. RADIO, Oct. 26, 2007, http://www.npr.org/templates/story/story.php?storyId=15673544.

24. *Id.*

25. ACLU of Northern California, 2006 Public Records Survey Summary Findings, http://www.aclunc.org/docs/government_surveillance/report_spreadsheet_for_web.pdf (last visited April 18, 2008) [hereinafter Public Records Summary].

26. Ryan Blitstein, *Cisco to Buy Surveillance Software Firm BroadWare*, SAN JOSE MERCURY NEWS, May 23, 2007.

27. Rick Coca, *Cops Seek More Surveillance Cameras*, DAILY NEWS, Jan. 22, 2008, at 1A.

28. Blitstein, *supra* note 26.

29. Anne Dudley Ellis, *School Teaches Video Security Design*, FRESNO BEE, Apr. 13, 2007, at B2.

30. *See* Katz v. United States, 389 U.S. 347 (1967). This definition of private places, like so many others, is imperfect. DANIEL J. SOLOVE ET AL., INFORMATION PRIVACY LAW 41 (2d ed. 2006) ("[D]efining privacy has proven to be quite complicated, and many commentators have expressed great difficulty in defining precisely what privacy is.").

out to be a private activity."[31] There is no federal or state legislation governing police video surveillance of public places.[32] Nor have courts imposed clear constraints. They have held that individuals can expect to be videotaped in or on streets,[33] sidewalks,[34] taverns,[35] front yards,[36] hallways at self-storage facilities,[37] mountaintops,[38] open fields,[39] and the common areas in public bathrooms.[40]

Few local governments have attempted to regulate video surveillance. Most large American police departments do not have written policies governing the use of video systems, according to one survey.[41] Another survey found that only about a quarter of California cities with video systems had written policies.[42] Relatively few cities may have policies in part because local officials generally believe that that the Fourth Amendment does not restrict video surveillance of public areas.[43] The Middleton, New York police department, for example, states in its policies that video sur-

---

31. Grant Fredericks, Consultant, Forensic Video Solutions, Gaining Pub. Support and Protecting Privacy Panel, Enhancing Public Safety Through Video Tech. Symposium, Int'l Ass'n of Chiefs of Police (Feb. 13, 2007).

32. Thomas D. Colbridge, *Electronic Surveillance: A Matter of Necessity*, FBI L. ENFORCEMENT BULL., Feb. 2000, at 26.

33. McCray v. State, 581 A.2d 45 (Md. Ct. Spec. App. 1990).

34. State v. Augafa, 992 P.2d 723 (Haw. Ct. App. 1999).

35. Sponick v. Detroit Police Dep't, 211 N.W.2d 674 (Mich. Ct. App. 1973).

36. State v. Holden, 964 P.2d 318 (Utah Ct. App. 1998).

37. State v. Bailey, 2001 Del. Super. LEXIS 471 (Del. Super. Ct. Nov. 30, 2001).

38. United States v. Sherman, No. 92-30067, 1993 U.S. App. LEXIS 6011 (9th Cir. Mar. 13, 1993).

39. State v. Costin, 720 A.2d 866 (Vt. 1998).

40. People v. Lynch, 445 N.W.2d 803 (Mich. Ct. App. 1989).

41. *See* Thomas J. Nestel III, Using Surveillance Camera Systems to Monitor Public Domains: Can Abuse Be Prevented? 27-44 (Mar. 2006) (unpublished thesis, Naval Postgraduate School) (on file with author).

42. Public Records Summary, *supra* note 25.

43. *See, e.g.*, Richard W. Chace, Serv. Indus. Ass'n, An Overview on the Guidelines for Closed Circuit Television (CCTV) for Public Safety and Community Policing 6 (2001), http://www.siaonline.org/research/privacy_guidelines_overview.pdf; Colbridge, *supra* note 32, at 25; Gary S. McLane, What Will Be the Impact of Video Surveillance in Public Areas by Mid-Sized Urban Agencies by 2007?, at 3 (June 2002) (unpublished project presented to the Command College Class at the California Commission on Peace Officer Standards and Training (POST)) (on file with POST Library, Sacramento, Cal.); Carl M. Miller, How Will the Implementation of Wireless Video Technology Impact Small Law Enforcement Agencies by 2007?, at 14 (June 2002) (unpublished project presented to the Command College Class at the California Commission on Peace Officer Standards and Training (POST)) (on file with POST Library, Sacramento, Cal.) ("[C]ritics notwithstanding, video surveillance devices in public do not seem to violate any constitutional principles.").

veillance "does not intrude upon an individual's sphere of privacy, but rather records events occurring in public space for which individuals do not have a reasonable expectation of privacy."[44] Similarly, Chicago Mayor Richard Daley has said that his city's state-of-the-art system does not compromise legitimate privacy rights by monitoring public spaces: "The city owns the sidewalk. We own the street and we own the alley."[45]

C. Lack of Regulation Poses a Threat of Misuse

Police have praised video surveillance as an effective tool.[46] They have said that surveillance systems have helped them deter and investigate crimes.[47] They have credited cameras with leading to the arrest of terrorist bombers in Oklahoma City[48] and London.[49] They have claimed that surveillance systems can help catch police engaged in wrongdoing and exonerate those falsely accused.[50] They have argued that installing video systems costs less than stationing officers at every corner.[51]

Observers have warned that no matter what its virtues may be, video surveillance also poses a threat. "Every court" that has considered the issue, according to Ninth Circuit Judge Alex Kozinski, has noted that "video surveillance can result in extraordinarily serious intrusions into personal

---

44. City of Middletown Police Dep't., Public Camera Policy and Procedure, http://www.middletownpolice.com/cameramain.htm (last visited Feb. 15, 2008).

45. Richard Roeper, *Smile, You're on Camera—and It Cleaned up Your Act*, CHI. SUN-TIMES, Sept. 13, 2004, at 11.

46. *E.g.*, Remarks of Robert Keyes, Interim Police Chief of Clovis, Cal., at the U.S. Dep't of Homeland Security Public Workshop—CCTV: Developing Privacy Best Practices, Law Enforcement Perspectives Panel 6-8 (Dec. 17, 2007) *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_workshop_cctv_Transcript_Law%20Enforcement_Perspectives_Panel.pdf (describing the effectiveness of his city's surveillance system).

47. *See, e.g.*, Alameda County District Attorney's Office, *Police Surveillance*, POINT OF VIEW, Winter 2007, at 1; Tobin Hensgen, *Video Makes the Case*, L. ENFORCEMENT TECH., Sept. 1, 2007, at 54.

48. Barbara Bell, *Waukegan Police Set to Install Surveillance Cameras*, CHI. TRIB., Aug. 15, 2005, at CN2; Miller, *supra* note 43, at 14.

49. *See, e.g.*, Clark Kent Ervin, *Surveillance Cameras Strike Balance in Fight Against Terrorism*, BALT. SUN, Aug. 5, 2007, at 15A; Alexandra Marks, *Should US Cities Try a London Style Camera Network?*, CHRISTIAN SCI. MONITOR, July 11, 2007, at 1.

50. Miller, *supra* note 43, at 27, 29.

51. *E.g.*, Paul Davis, *Technology Serves as Force Multiplier*, L. ENFORCEMENT TECH., June 1, 2007, at 28; Max Marbut, *Someone's Watching You*, JACKSONVILLE DAILY REC., Mar. 7, 2008, http://www.jaxdailyrecord.com/showstory.php?Story_id=49590 (quoting an officer as saying that "[t]he video system is very cost-effective . . . Remote control cameras are expensive, but they are a one-time cost. Here at the Main Library, I would need 12 more security officers to cover the building if we didn't have the video system.").

privacy."[52] Michigan Governor Jennifer Granholm, before beginning her political career, wrote that "even the most tenacious prosecutor would admit that there is an 'Orwellian odor' to camera surveillance on public street corners."[53] The ACLU—perhaps the most vocal and visible opponent of video surveillance—has argued that video systems "infringe on the freedom of speech and association guaranteed by the First Amendment and threaten the anonymity and privacy protected by the Fourth."[54]

The sophistication of new video systems amplifies these concerns.[55] The technological constraints that prevented misuse of analog surveillance cameras—grainy images, limited storage capacity, and difficult duplication—no longer impede video surveillance.[56] In the way that the digital revolution has allowed consumers to easily distribute, download, and edit movies and songs, it has allowed police to do the same with surveillance footage. Such unbounded abilities could aid in investigations and prosecutions but could also allow system users to tamper with evidence or engage in voyeuristic behavior.

---

52. United States v. Kouyoumejian, 970 F.2d 536, 551 (9th. Cir. 1992) (Kozinski, J., concurring).

53. Jennifer Mulhern Granholm, *Video Surveillance on Public Streets: the Constitutionality of Invisible Citizen Searches*, 64 U. DET. L. REV. 687, 689 (1987).

54. MARK SCHLOSBERG & NICOLE A. OZER, CALIFORNIA ACLU OF NORTHERN CAL., UNDER THE WATCHFUL EYE: THE PROLIFERATION OF VIDEO SURVEILLANCE SYSTEMS IN CALIFORNIA 7-8 (2007), *available at* http://www.aclunc.org/docs/criminal_justice/police_practices/Under_the_Watchful_Eye_The_Proliferation_of_Video_Surveillance_Systems_in_California.pdf. Meanwhile, the New York-based performance art group Surveillance Camera Players has earned notoriety for staging short plays in front of surveillance cameras. Sabrina Tavernise, *Watching Big Brother; On this Tour, Hidden Cameras are Hidden No More*, N.Y. Times, Jan. 17, 2004, at B1.

55. *See, e.g.*, Kevin Fagan, *Surveillance Foes Renew their Battle*, S.F. CHRON., Aug. 18, 2007, at A1; Rich Lord, *Network of Surveillance Cameras Proposed*, PITT. POST-GAZETTE, June 27, 2007, at B1; Myron P. Medcalf, *Police to Put Cameras on St. Paul's Central Corridor; City Council Approval Will Mean $1.2 Million to Place 60 Cameras Along University Avenue and in Downtown*, MINNEAPOLIS STAR TRIB., Aug. 4, 2007, at 5B.

56. *See* CONSTITUTION PROJECT, *supra* note 11, at 4-6 (describing technological improvements in video surveillance technology).

Privacy activists have pointed to a variety of potential threats.[57] At a basic level, those in control of surveillance cameras could zoom in on attractive women or track individuals because of their race.[58] At a more sophisticated level, hackers could break into wireless networks and hijack police cameras.[59] License plate readers could link information about the geographic movement of cars to private data like the insurance records of car owners.[60] Police could monitor attendance at political rallies, abortion or HIV clinics; they could read books or letters over the shoulders of commuters waiting for the next bus. Such surveillance—undetectable, unrelenting, and unchecked—could lead to the collection of large amounts of sensitive information and could change the public character of our society.[61]

This threat is real. Consider the story of Paris Lane. In 2004, a police surveillance video captured twenty-two year old Lane killing himself in the lobby of a Bronx public housing unit.[62] A New York City police officer e-mailed a clip of the suicide to a friend,[63] and the footage ultimately found its way to a shock website. The website described the clip—which

57. *See* COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER TO DEPARTMENT OF HOMELAND SECURITY ON DOCKET NO. DHS-2007-0076 (2008), *available at* http://epic.org/privacy/surveillance/epic_cctv_011508.pdf; SCHLOSBERG & OZER, *supra* note 54; NEW YORK CIVIL LIBERTIES UNION, WHO'S WATCHING: VIDEO CAMERA SURVEILLANCE IN NEW YORK CITY AND THE NEED FOR PUBLIC OVERSIGHT 7-12 (2006), http://www.nyclu.org/pdfs/surveillance_cams_report_121306.pdf; Deirdre K. Mulligan, Director, Samuelson Law, Tech. & Pub. Pol'y Clinic, UC Berkeley School of Law (Boalt Hall), In Defense of Public Spaces, Statement Before the Department of Homeland Security Data Privacy and Integrity Advisory Committee (June 7, 2006), *available at* http://groups.ischool.berkeley.edu/samuelsonclinic/files/Mulligan_DHS_ Statement.pdf ; AM. BAR ASS'N, STANDARDS FOR CRIMINAL JUSTICE: ELECTRONIC SURVEILLANCE sec. B, at 23 (3d ed. 1998), *available at* http://www.abanet.org/crimjust/standards/electronicsectionb.pdf.

58. Nestel, *supra* note 41, at 6-8 (citing instances in which casino employees and peace officers have used cameras to view women's breasts and buttocks).

59. Bob Pool, *Two Accused of Sabotaging Traffic Lights*, L.A. TIMES, Jan. 6, 2007, at B1.

60. Remarks of Clive Norris, Professor of Sociology at the University of Sheffield and Deputy Director of the Center for Criminological Research, at the U.S. Dep't. of Homeland Security Public Workshop—CCTV: Developing Privacy Best Practices, International Perspectives Panel 18-19 (Dec. 17, 2007), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_workshop_cctv_Transcript_International_Perspectives_ Panel.pdf.

61. Mulligan, *supra* note 57.

62. Shaila K. Dewan, *Video of Suicide in Bronx Appears on Shock Web Site*, N.Y. TIMES, Apr. 1, 2004, at B3.

63. Murray Weiss, *Bx. Cop Caught in 'Net—Suicide-Video Scandal*, N.Y. POST, June 22, 2004, at 25.

showed Lane saying good-bye to a tearful woman before shooting himself in the face with a nine-millimeter handgun—as the "Self-Cleansing Housing Projects."[64] Police did not learn of the leak until Lane's foster mother contacted them.[65] Before the advent of digital technology,[66] computer users could not easily upload, copy, and e-mail flawless copies. Now, though, few obstacles prevent bored or reckless monitors from releasing such footage, and even fewer obstacles prevent those monitors from zooming in on a bedroom or following a woman down the street.[67]

It is possible that few stories like that of Paris Lane have come to light because police misuse of video systems is difficult to detect.[68] Video systems make no noise and leave no physical trace. An officer may track a suspect or e-mail footage of that suspect to a friend without the suspect, much less his neighbors, ever knowing. The public would not have learned about the Paris Lane leak if a website had not posted the footage, if friends had not told Lane's foster mother about the posting, and if Lane's foster mother had not complained.

D. Need for Regulation

Regulation could prevent the misuse and ineffective use of video systems in three respects. First, regulation could shape the conduct of those officers who might be inclined to use video systems in ways that are unethical but not illegal. Regulation could clearly define the scope of permissible activities and remove ambiguity as to what conduct the law prohibits. Officers would not have to rely on their own sense of what is appropriate but could instead rely on the express guidance of regulatory rules.

Second, regulation could ensure accountability by attaching consequences to certain acts. Such consequences could provide monitors and operators with incentives for acting or not acting in particular ways: the greater the positive consequences, the greater the incentive to avoid misuse. If monitors understood that they could be disciplined for using video

64. Dewan, *supra* note 62, at B3.

65. *Id.*

66. *See* discussion *supra* Section II.A on analog video surveillance.

67. In another infamous incident, a camera-equipped New York City police helicopter that was supposed to be monitoring a mass bicycle ride through Lower Manhattan recorded a couple being intimate on a rooftop balcony. The recoding became public when it was used in the trial of a cyclist and, eventually, the local CBS station aired it during a news broadcast. Police supervisors and the public would not have known that officers were using the cameras to watch the couple if not for an unrelated lawsuit. Jim Dwyer, *Police Video Caught a Couple's Intimate Moment on a Manhattan Rooftop*, N.Y. TIMES, Dec. 22, 2005, at B10.

68. Mulligan, *supra* note 57, at 2.

systems to track the movements of ex-girlfriends or fired for e-mailing sensitive footage to friends, they would have a strong reason not to do so.

Third, regulation could define behavioral standards. It could encourage the development of professional customs that incorporate best practices and create a working environment that promotes the responsible and efficient use of video systems.[69] Studies have found, for example, that officers have trouble concentrating on surveillance monitors—especially multiple ones—for more than twenty minutes.[70] Regulation that discourages officers from spending an extended period of time in front of monitors, except in exigent circumstances, could help officers to avoid the kinds of situations where they might be more inclined to use video systems improperly.

III. INADEQUACY OF JUDICIAL REGULATION

This Part: A) briefly reviews the judicial laws that apply to warrantless video surveillance of public places; B) focuses on the Fourth Amendment, which imposes the most significant limits upon video surveillance; and C) concludes that unless the Supreme Court amends the framework set forth in *Katz v. United States*, governments at all levels will continue to invest in video systems that erode privacy rights but that do not implicate existing Fourth Amendment rules.

A. Overview: Judicial Limitations

Video surveillance could implicate the First[71] and Fourth[72] Amendments and the Due Process[73] and Equal Protection[74] clauses of the Fourteenth Amendment.[75] If police used video systems to monitor and suppress

---

69. *See infra* Part VI (discussing the interplay between law and custom).

70. NAT'L INST. OF JUSTICE, THE APPROPRIATE AND EFFECTIVE USE OF SECURITY TECHNOLOGIES IN U.S. SCHOOLS: A GUIDE FOR SCHOOLS AND LAW ENFORCEMENT AGENCIES 30 (1999) (discussing studies that show that "[a]fter only 20 minutes of watching and evaluating monitor screens, the attention of most individuals has degenerated to well below acceptable levels").

71. U.S. CONST. amend. I ("Congress shall make no law . . . abridging the freedom of speech . . . or the right of the people peaceably to assemble.").

72. U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause.").

73. U.S. CONST. amend. XIV § 1 ("... nor shall any State deprive any person of life, liberty, property without due process of law.").

74. U.S. CONST. amend. XIV § 1 ("No State shall . . . deny to any person within its jurisdiction the equal protection of the laws.").

75. Remarks of Chris Slobogin, Professor of Law, University of Florida Levin College of Law, at the U.S. Dep't. of Homeland Security Public Workshop—CCTV: Developing Privacy Best Practices, Legal and Policy Perspectives Panel 2, 6 (Dec. 18, 2007),

expressions of free speech, courts might find such use has a First Amendment chilling effect.[76] If police used the systems to interfere with an individuals' right to travel and repose, courts might find a Due Process violation; and if police used the systems to discriminate against protected classes, courts might an Equal Protection violation.[77] Certain kinds of video surveillance might also violate the privacy provisions found in some state constitutions. More centrally, the source of judicial oversight of video surveillance of public areas is the Fourth Amendment.[78]

B. Recognized Fourth Amendment Limits

The Supreme Court has considered the Fourth Amendment implications of the police use of tracking beepers,[79] electronic eavesdropping devices,[80] photographic cameras with zoom lenses,[81] and thermal-imaging devices,[82] but not the use of video surveillance systems. Seven circuit courts have considered the use of cameras in private places like offices and homes, but none have directly addressed the use in public places like street corners and parks.[83] The prevailing opinion in the legal community

---

available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_workshop_cctv_Transcript_Legal _and_Policy_Perspectives_ Panel.pdf.

76. *E.g.*, Dombrowski v. Pfister, 380 U.S. 479, 487 (1965) ("The chilling effect upon the exercise of First Amendment rights may derive from the fact of the prosecution, unaffected by the prospects of its success or failure."). Current uses seem unlikely to trigger a chilling effect, however. *See* Watchtower Bible & Tract Soc'y of N.Y., Inc. v. Vill. of Stratton, 536 U.S. 150, 163 (2002) ("[T]here must be a balance between these interests and the effect of the regulations on First Amendment rights. We must be astute to examine the effect of the challenged legislation and must weigh the circumstances and . . . appraise the substantiality of the reasons advanced in support of the regulation."); Laird v. Tatum, 408 U.S. 1, 13 (1972) ("Allegations of a subjective 'chill' are not an adequate substitute for a claim of specific present objective harm or a threat of specific future harm.").

77. Slobogin, *supra* note 75, at 6.

78. *Id.* at 2.

79. United States v. Karo, 468 U.S. 705 (1984); United States v. Knotts, 460 U.S. 276 (1982).

80. Katz v. United States, 389 U.S. 347 (1967).

81. Dow Chemical Co. v. United States, 476 U.S. 227 (1985).

82. Kyllo v. United States, 533 U.S. 27 (2001).

83. United States v. Williams, 124 F.3d 411 (3d Cir. 1997); United States v. Falls, 34 F.3d 674 (8th Cir. 1994); United States v. Taketa, 923 F.2d 665 (9th Cir. 1991); United States v. Mesa-Rincon, 911 F.2d 1433 (10th Cir. 1990); United States v. Cuevas-Sanchez, 821 F.2d 248 (5th Cir. 1987); United States v. Biasucci, 786 F.2d 504 (2d Cir. 1986); United States v. Torres, 751 F.2d 875 (7th Cir. 1984). In one unpublished decision, however, the Ninth Circuit did rule that individuals could not reasonably expect not to be videotaped as they sold drugs on mountain passes. United States v. Sherman, No. 92-30067, 1993 U.S. App. LEXIS 6011 (9th Cir. Mar. 13, 1993).

is that video systems do not violate the Fourth Amendment when cameras monitor public places because the plain view doctrine applies to whatever activity occurs in those places.[84] Fourth Amendment doctrine suggests, though, that there are three limits to the application of the plain-view doctrine to video surveillance: 1) police cannot use cameras posted in public places to monitor places where there is an expectation of privacy; 2) police cannot use zoom lenses to magnify individuals or their belongings to a degree that is invasive; and 3) police cannot use cameras on such a broad scale as to conduct mass searches without suspicion.

1. Monitoring Places Where There is an Expectation of Privacy

Police cannot use video systems to engage in warrantless surveillance of places where there is an expectation of privacy,[85] but it is difficult to identify which places have expectations of privacy. The Supreme Court held in *Katz v. United States* that "the Fourth Amendment protects people, not places."[86] Fourth Amendment protection attaches, according to the *Katz* Court, if two conditions are met: 1) an individual must have an expectation of privacy; and 2) society must recognize that expectation as reasonable.[87] Since individuals can always claim to have expectations of privacy, courts have generally focused on whether society—or, more realistically, presiding judges[88]—recognizes those expectations as reasonable.

Courts have generally held that what people do in public is exposed to plain view and that people do not have reasonable privacy expectations in what they expose to plain view.[89] But courts have split over the exact lim-

84. If the video system records conversations, however, it could violate the prohibition against warrantless electronic eavesdropping under the Wiretap Act. Ric Simmons, *Technology-Enhanced Surveillance by Law Enforcement Officials*, 60 N.Y.U. ANN. SURV. AM. L. 711, 725 n.46 (2005). So far, municipalities have not equipped their systems with such audio recording devices; however, a number have outfitted their systems with Shotspotter, which triangulates sounds to identify the location of gunshots. Shotspotter, Customers Overview, http://www.shotspotter.com/customers/index.html (last visited Jan. 8, 2008).

85. *Torres*, 751 F.2d at 875.

86. Katz v. United States, 389 U.S. 347, 351 (1967).

87. *Id.* at 361 (Harlan, J., concurring).

88. *See* Minnesota v. Carter, 525 U.S. 83, 97 (1998) (Scalia, J., concurring) ("In my view, the only thing the past three decades have established about the *Katz* test . . . is that, unsurprisingly, those 'actual (subjective) expectations of privacy' 'that society is prepared to recognize as "reasonable,"' bear an uncanny resemblance to those expectations of privacy that this Court considers reasonable.").

89. Kyllo v. United States, 533 U.S. 27, 37 (2001) ("In the home, our cases show, *all* details are intimate details, because the entire area is held safe from prying government eyes.").

its of the plain view doctrine.[90] One notable split is over the right of police to peer through house or apartment windows. Out of respect for this legal gray area, or maybe respect for community concerns about privacy, some police departments have digitally masked views of sensitive places like home windows or have stationed cameras or limited their tilting abilities so that they cannot look into those places.[91]

Courts have hinted that the plain view doctrine might operate like a sliding scale, with some things only partly in plain view and others completely in plain view. The Sixth Circuit recently held that students, even though they are among others, can reasonably expect not to be videotaped in school locker rooms.[92] The Ninth Circuit reached a similar holding regarding police officers in a station locker room.[93] The Fifth Circuit has held that individuals cannot expect police or members of the public not to see into their backyards when flying overhead,[94] but they can expect that no one will monitor their backyards with video cameras for extended peri-

90. Some courts have held that individuals cannot reasonably expect police not to view them through their home windows. People v. Wright, 242 N.E.2d 180 (Ill. 1968) (finding that an officer standing on a public transit authority right of way did not violate the Fourth Amendment when he looked through the curtains of a nearby window); Commonwealth v. Busfield, 363 A.2d 1227 (Pa. Super. Ct. 1976) (finding that police did not violate a reasonable expectation of privacy when looking through sheer curtains from the neighboring property). Other courts have found that individuals can reasonably expect for officers not to view them through their home windows. *Carter*, 525 U.S. at 83 (finding that a police officer would have violated the Fourth Amendment rights of respondents by peering through a drawn window blind if the respondents had had standing); United States v. Taborda, 635 F.2d 131 (2d Cir. 1980) (police violated Fourth Amendment rights by not obtaining a warrant before using a telescope to see into an apartment). *See also* People v. Henderson, 220 Cal. App. 3d 1632, 1649 (Cal. Ct. App. 1990) ("The plain and simple fact is clandestine observations into a private residence from a vantage point inaccessible to the public or an uninvited guest is a search which, if conducted without a warrant, is the type of activity the Fourth Amendment proscribes."); Raettig v. State, 406 So.2d 1273 (Fla. Dist. App. 1981) (finding that police violated Fourth Amendment privacy rights by using a flashlight to peer through a "minute crack on the surface" of a camper); State v. Ward, 617 P.2d 568 (Hawaii 1980) (finding that police violated constitutional privacy rights by using binoculars to watch a craps game being played in a seventh floor apartment, an eighth of a mile away).

91. *See* SAMUELSON LAW, TECH. & PUB. POL'Y CLINIC, UC BERKELEY SCHOOL OF LAW (BOALT HALL), POLICIES AND PROCEDURES COMPARED (Dec. 2008) (unpublished analysis of collected policies and procedures) (on file with the Samuelson Law, Technology, and Public Policy Clinic at UC Berkeley School of Law).

92. Brannum v. Overton County Sch. Bd., 516 F.3d 489 (6th Cir. 2008).

93. Bernhard v. City of Ontario, No. 06-55736, 2008 WL 687352 (9th Cir. Mar. 13, 2008).

94. Florida v. Riley, 488 U.S. 445 (1989); California v. Ciraolo, 476 U.S. 207 (1986).

ods of time.[95] Video surveillance, the court found, was more invasive than "a one-time overhead flight or a glance over the fence by a passer-by."[96]

2. Invasive Zooming

In *Dow Chemical Co. v. United States*, the Supreme Court addressed a particularly advanced form of telescopic surveillance and found that police did not violate the Fourth Amendment when they flew an airplane over a chemical plant and used a $22,000 mapmaking camera to photograph the facilities.[97] The *Dow* Court did not give blanket approval to the warrantless use of all zoom devices, but it indicated that at a certain level of magnification, zooming would be so invasive as to require a warrant. It observed that the *Dow* photographs did not capture "objects as small as 1/2-inch in diameter such as a class ring" or "identifiable human faces" or "secret documents."[98] The Court might have ruled differently, this observation suggests, if the photographer had zoomed in so far that the camera recorded small or sensitive details.

3. Mass Searches Without Suspicion

Courts have hinted that mass suspicion-less searches might violate the Fourth Amendment. So far, video surveillance cases have concerned cameras that did not have the technological ability to conduct mass searches. Increasingly, though, cities are deploying integrated systems that—if sufficiently invasive, far-seeing and unrelenting—could conduct mass searches and implicate the Fourth Amendment.

In a case involving a tracking beeper,[99] the Supreme Court distinguished between individual beepers and integrated surveillance networks. The Court suggested that systems that allow for "twenty-four hour surveillance of any citizen in this country" and "dragnet-type law enforcement practices" could raise Fourth Amendment concerns.[100] The Seventh Circuit, in turn, recently opined that "[t]echnological progress poses a threat to privacy by enabling an extent of surveillance that in earlier times would have been prohibitively expensive" and that, "[s]hould government someday decide to institute programs of mass surveillance of vehicular movements," courts must consider whether such surveillance constitutes a

95. United States v. Cuevas-Sanchez, 821 F.2d 248 (5th Cir. 1987)

96. *Id.* at 251.

97. Dow Chemical Co. v. United States, 476 U.S. 227, 251 n.13 (1985).

98. *Id.* at 238 n.5.

99. United States v. Knotts, 460 U.S. 276, 277 (1983) ("A beeper is a radio transmitter, usually battery operated, which emits periodic signals that can be picked up by a radio receiver.").

100. *Id.* at 283-84.

Fourth Amendment search.[101] Despite significant advances in video surveillance, there are few if any video systems in this country that could conduct the kind of mass searches without suspicion that courts have disavowed. Video systems connected to license plate readers could serve as the foundation for "programs of mass surveillance of vehicular movements," but even those seem unlikely to trigger current Fourth Amendment rules, since courts have already accepted the legality of devices that can monitor the movements of particular vehicles.[102]

C. Video Surveillance and the *Katz* Framework

Even if municipalities deployed the kinds of video systems that pushed Fourth Amendment limits, considerable time could pass before the Supreme Court heard and decided a case regarding the constitutionality of video surveillance of public places. One of the general disadvantages of case law is that it is slow to develop, and that is as true in the context of electronic surveillance as in any other area of the law. Americans had been using wiretaps for more than sixty years before the Supreme Court heard a wiretapping case;[103] and almost forty more years passed before the Court ruled that warrantless wiretapping violated the Fourth Amendment.[104] Britain developed its video surveillance infrastructure in less than ten years,[105] and if the Court takes longer than that to decide a case on the video surveillance of public places, then its decision will probably have to account for the fact that cities across the country have already installed expensive video systems.

Still, the Supreme Court could revisit its Fourth Amendment privacy jurisprudence and either modify *Katz* or replace it with a rule better suited to the technologies that have developed in the past forty years. The *Katz* rule, which encourages courts to determine the reasonableness of privacy expectations on the basis of place, seems to offer no protection against invasive new technologies if those technologies are used in public places. *Katz* claims that the Fourth Amendment "protects people, not places," but

101. United States v. Garcia, 474 F.3d 994, 998 (7th Cir. 2007).

102. *Id.* at 994; Buliga v. N.Y. City Taxi Limousine Comm'n, 07-CV-6507, 2007 U.S. Dist. LEXIS 94024 (S.D.N.Y. Dec. 21, 2007); Morton v. Nassau County Police Dep't, 05-CV-4000, 2007 U.S. Dist. LEXIS 87558 (E.D.N.Y. Nov. 27, 2007).

103. Michael Goldsmith, *The Supreme Court and Title III: Rewriting the Law of Electronic Surveillance*, 74 J. CRIM. L. & CRIMINOLOGY 1, 3-4 (1983).

104. Berger v. New York, 388 U.S. 41 (1967).

105. Remarks of Larry Strach, V.P. of Eng'g, Duos Technologies, at the U.S. Dep't. of Homeland Security Public Workshop—CCTV: Developing Privacy Best Practices, Technology Perspectives Panel 17 (Dec. 17, 2007) , *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_workshop_cctv_Transcript_Technology_Perspectives_Panel.pdf.

it establishes a rule that effectively elevates place above other factors when considering the reasonableness of a privacy expectation.

Katz has had many critics,[106] and few commentators have seemed particularly pleased with the most recent opinion in the *Katz* line of cases, *Kyllo v. United States*.[107] *Kyllo* established a rule that police must obtain warrants to use sense-enhancing technologies[108] that are not in "general public use"[109] to monitor the insides of homes, but so far this rule has failed to provide much practical guidance.[110] Meanwhile, other technologies have begun to strain the *Katz* framework and could ultimately compel the Court to reconsider the *Katz* rule. Deirdre Mulligan and Jack Lerner have argued, for instance, that digital-electricity usage readings could reveal intimate details about activities inside homes, like at what times individuals go to sleep and work and what kinds of appliances they use, and that such readings might give rise to litigation that forces courts to recon-

106. A common critique is that *Katz* sets forth a subjective and circular test. David A. Sklansky, *Back to the Future:* Kyllo, Katz, *and Common Law*, 72 MISS. L.J. 143, 158 (2002) ("But how are judges to tell whether society is in fact 'prepared to recognize' an expectation as 'reasonable'? The inquiry has proved distressingly indeterminate, and many observers, on and off the Court, have thought it circular: an expectation of privacy is reasonable if the Court is willing to protect it."); Anthony Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 384 (1974) (explaining that if Fourth Amendment privacy protection did depend on subjective expectations of privacy, "the government could diminish each person's subjective expectation of privacy merely by announcing half-hourly on television . . . that we were all forthwith being placed under comprehensive electronic surveillance"); *see also* Bailey H. Kuklin, *The Plausibility of Legally Protecting Reasonable Expectations*, 32 VAL. U. L. REV. 19 (1997); Robert Morris, *Some Notes on Reliance*, 75 MINN. L. REV. 815 (1991).

107. Kyllo v. United States, 533 U.S. 27 (2001). *See* Daniel McKenzie, Note, *What Were They Smoking?: The Supreme Court's Latest Step in a Long, Strange Trip Through the Fourth Amendment*, 93 J. CRIM. L. & CRIMINOLOGY 153 (2002); Richard H. Seamon, Kyllo v. United States *and the Partial Ascendance of Justice Scalia's Fourth Amendment*, 79 WASH. U. L.Q. 1013, 1022 (2001) ("[T]he *Kyllo* majority did not apply the Katz test to the case before it.").

108. The Supreme Court has defined sense-enhancing technologies as devices that aid police in "augmenting the sensory faculties bestowed upon them at birth." United States v. Knotts, 460 U.S. 276, 284 (1983).

109. *Kyllo*, 533 U.S. at 34.

110. The rule raises questions about what constitutes general public use. The Court held "that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area,' constitutes a search—at least where (as here) the technology in question is not in general public use." *Id.* at 34. The Court did not define "general public use" or provide any rule for determining when a technology is in general public use.

sider the third party doctrine[111] that has developed from *Katz* and perhaps even *Katz* itself.[112] Such technologies could readily reveal the type of information about domestic activities that *Kyllo* professed to protect—that is, "details of the home that would previously have been unknowable without physical intrusion."[113]

IV. NATIONAL AND STATE LEGISLATIVE REGULATION

This Part argues that: A) Congress should pass legislation regulating video surveillance; B) this legislation could build upon the privacy protections established under the E-Government Act; and C) states should consider legislation that addresses state-level concerns related to video surveillance and that provides guidance in the absence of federal legislation.

A. Congressional Legislation

There are two reasons why Congress should regulate video surveillance. The first is that federal funding has encouraged and accelerated the adoption of video systems. The federal government should therefore impose accountability on its use.[114] The second reason is that video surveillance raises national concerns.

The federal government has helped numerous local governments fund video systems.[115] According to one estimate, the DHS alone has distrib-

111. The third party doctrine provides that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." Smith v. Maryland, 442 U.S. 735, 743-44 (1979).

112. Deirdre K. Mulligan & Jack Lerner, *Taking the "Long View" on the Fourth Amendment: Stored Records and the Sanctity of the Home*, 2007 STAN. TECH. L. REV. 3, 10 (2007) ("The cultural dependence on private sector services that generate records containing personal information about activities occurring within the home are blurring the "firm line" around the home that the founders sought to protect. But it is just one example in a growing list. The Court's disjointed approach to dataveillance and surveillance cannot sustain the privacy of the home as the framers' or the current court envisioned it.").

113. *Kyllo*, 533 U.S. at 40.

114. Charlie Savage, *US Doles Out Millions for Street Cameras; Local Efforts Raise Privacy Alarms*, BOSTON GLOBE, Aug. 12, 2007, at A1.

115. *Id.*; *see also* Tomas Alex Tizon, *Eighty Eyes on 2,400 People; If Terrorists Come to Tiny Dillingham, Alaska, Security Cameras Will be Ready. But Privacy Concerns Have Residents Up in Arms*, L.A. TIMES, Mar. 28, 2006, at A1 (explaining how DHS grants funded eighty cameras for a town of 2,400). But others have funded systems without federal help. *See, e.g.*, Tami Abdollah, *Wanna be in Pictures? Tag in Montebello*, L.A. TIMES, Nov. 15, 2007, at B2; Mark McDonald, *$5M Earmarked for Photo Surveillance*, PHILA. DAILY NEWS, Feb. 2, 2007 Local 08; Norberto Santana Jr., *National City Likely to Push for Bond*, SAN DIEGO UNION-TRIBUNE, May 29, 2004, at B1.

uted about $230 million in video surveillance grants.[116] These grants have directly funded systems in some cities and have encouraged other cities to consider installing video systems.[117] In certain instances, the DHS grants have paid to install cameras at critical infrastructure[118] sites and local governments have themselves paid to extend the video system to other sites.[119] Some grants have helped to fund elaborate big-city systems. For example, the "first its kind"[120] Lower Manhattan Security Initiative, a dense system of license plate readers and public and private cameras,[121] has attracted attention from press across the country[122] and from the law enforcement community.[123]

Federal funding may have also indirectly encouraged cities to install video systems. Once one city has a video system and word of the system begins to travel, other cities may begin to consider installing similar systems. The initial city serves as an early-adopter and maybe even a trendsetter. A visit to Chicago, for instance, inspired San Francisco Mayor Gavin Newsom to install cameras in his city.[124] The studies that have examined the impact of video systems have found the systems to have less effect on crime than alternative policing methods—like more beat officers

116. COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER, *supra* note 57, at 2-3 (citing correspondence from Toby Levin, Senior Advisor, DHS Privacy Office as the source of this figure).

117. Savage, *supra* note 114. *See also* Rich Lord, *City Eyes Widened Security Camera Coverage*, PITT. POST-GAZETTE, Jan. 1, 2008, at B1; Larry Sandler, *City Camera Funding Rejected*, MILWAUKEE J. SENTINEL, June 14, 2007, at B1; Matt Stiles et al., *HPD Wants Cameras to Monitor Crime*, HOUS. CHRON., May 15, 2007, at A1;

118. *See* USA PATRIOT Act of 2001, 42 U.S.C. § 5195(c)(e) (Supp. II 2002) (defining critical infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.").

119. *E.g.*, City of Richmond, Cal., City Council Agenda, at 5, item D (July 31, 2007).

120. *Cameras and Crime*, N.Y. POST, July 11, 2007, at 28.

121. Cara Buckley, *Police Plan Web of Surveillance for Downtown*, N.Y. TIMES, July 9, 2007, at A1.

122. *See, e.g.*, *New York Plans Heightened Security Network*, GRAND RAPIDS PRESS, Sept. 9, 2007, at G4; *Cameras to Watch Wall St., Environs*, L.A. TIMES, Sept. 7, 2007, at A27; *The Issue: Surveillance; Security Cameras Fight Terror*, ARIZ. REPUBLIC, July 15, 2007, Opinions, at 4.

123. *See, e.g.*, Linda Spagnoli, NYC Fights and WiNs! New York City Applies DHS Funding to Create the Citywide Mobile Network NYC WiN, L. ENFORCEMENT TECH., May 1, 2007, at 70.

124. Cecilia M. Vega, *Newsom Going to Big Apple for Climate Summit*, S.F. CHRON., Sept. 19, 2006, at B2.

or street lighting—that would cost the same amount of money.[125] But there are many anecdotes about the success of video systems.[126] These anecdotes—along with the visibility of early adopters, the availability of grant money, and the general desire to prevent terrorism and reduce crime—may have led some cities that would not have otherwise considered video systems to adopt them.[127] This combination of factors, in other words, may have skewed the incentives for video surveillance.[128]

If the federal government is directly or indirectly pushing local governments to adopt video systems, it should push them to do so prudently. The federal government already requires its agencies to assess the impact that new technologies like video surveillance will have on privacy rights. Federal grants that fund state purchases of surveillance technologies without also requiring states to assess the privacy impact could be creating a situation that permits states to "completely circumvent congressional will that the privacy effects of technology be understood and explored and mitigated."[129]

The second reason that Congress should pass regulatory legislation is that video surveillance raises issues of national concern. The federal government sets the national security agenda.[130] It has created a complex

125. SCHLOSBERG & OZER, *supra* note 54, at 11 ("Numerous studies of existing camera programs demonstrate that they do not significantly reduce crime, especially violent crime in city centers. Furthermore, expectations that surveillance cameras will significantly increase the success rate of criminal prosecutions have not been met.").

126. Marcus Baram, *Eye on the City: Do Cameras Reduce Crime*, ABC NEWS, July 9, 2007, http://abcnews.go.com/print?id=3360287 (quoting Int'l Ass'n of Chiefs of Police research director John Firman as saying: "We know that cameras enhance that capacity but saying for sure that they reduced crime by 20 percent, that's another thing. Anecdotally, we know that they have had an impact."); *see also* Paula Lloyd, *Police Set on Dismantling Gangs*, FRESNO BEE, Apr. 3, 2008 , at B4 (noting that police cameras captured a recent shooting); Scott Jason, *Chief Wants Surveillance to Discourage Theft, Graffiti*, MODESTO BEE, Feb. 21, 2007, at B01 (describing the impact that cameras have had on illegal graffiti in one California town).

127. *E.g.*, Larry Sandler, *National Ave. to Get Security Cameras*, MILWAUKEE J. SENTINEL, May 23, 2006, at A1 (discussing Milwaukee's efforts to establish a video system, which included applying for a federal grant and sending a police captain to Chicago to learn about the system there).

128. Remarks of Deidre K. Mulligan, Director, Samuelson Law, Tech. & Pub. Pol'y Clinic, UC Berkeley School of Law, at the U.S. Dep't. of Homeland Security Public Workshop—CCTV: Developing Privacy Best Practices, Panel on Developing Privacy Best Practices for the Use of CCTV 30 (Dec. 18, 2007).

129. *Id.*

130. *See* U.S. CONST. art. I, § 8, cl. 1, 10-12, art. II, § 2, cl. 1; Youngstown Sheet & Tube Co v. Sawyer, 343 U.S. 579 (1952).

statutory framework relating to surveillance and intelligence gathering.[131] This infrastructure includes statutes that govern the use of invasive surveillance technologies.[132] These statutes apply to wiretaps,[133] pen registers,[134] and trap-and-trace devices.[135] They do not apply to video surveillance.[136] The federal government is better positioned than lower levels of government to develop legislation that clarifies the way that video surveillance is supposed to advance the national security agenda and that explains the way that video surveillance should fit into the broader national security statutory framework.

Additionally, as video systems expand, they may take on an increasingly national character. They may even evolve into a national network similar to the American highway system or telecommunications grid.[137] The federal government could establish legal and technological standards that promote compatibility among systems and collaboration among the jurisdictions that use those systems.[138] The video systems in large cities, for instance, often consist of the overlapping systems run by agencies like the police department, the housing authority, and the transit authority. In the District of Columbia, for instance, the Metropolitan Police operate one camera system, and the National Park Police operate another.[139] In some large metropolitan areas, those systems will probably begin to stretch

131. SOLOVE, *supra* note 30, at 263-272.

132. *Id.*

133. Wiretap Act, 18 U.S.C. §§ 2510-22 (2000).

134. Pen Register Act, 18 U.S.C. §§ 3121-27 (2000).

135. *Id.*

136. SOLOVE, *supra* note 30, at 276-77.

137. The Australian government, for instance, has proposed a network of cameras and license plate readers that could form "the rudiments of a national monitoring network." Paul Maley, *Hi-tech Crime Cameras on Roads by Next Year*, Jan. 1, 2008, THE AUSTRALIAN, at Local 1.

138. *See* HOMELAND SEC. COUNCIL, NATIONAL STRATEGY FOR HOMELAND SECURITY 4 (2007) ("The National Government also is responsible for developing national strategies as well as promulgating best practices, national standards for homeland security, and national plans, as appropriate."); *see also* HOME OFFICE, NATIONAL CCTV STRATEGY (2007) (describing the importance of CCTV standards from the perspective of the British government); Council of Australian Governments (COAG), Special Meeting on Counter-Terrorism Communiqué (Sept. 27, 2005), http://www.coag.gov.au/meetings/270905/index.htm ("COAG also agreed to a national, risk-based approach to enhancing the use of CCTV for counter-terrorism purposes, including the development of a National Code of Practice for CCTV systems for the mass passenger transport sector. The Code will set a policy framework, objectives, protocols and minimum requirements.").

139. Law Enforcement Perspectives, *supra* note 46, at 10.

across state lines.[140] Given such circumstances, "a national strategy," as Senator Joe Lieberman has called it, could "help officials at the federal, state, and local levels use systems effectively to protect citizens, while at the same time making sure that appropriate civil liberties protections are implemented for the use of cameras and recorded data."[141]

B. Scope of Federal Legislation—Learning from the E-Government Act

The E-Government Act of 2002,[142] may offer a model for the type of legislation that could protect privacy interests without imposing undue burdens or restrictions on lower levels of government for video surveillance.

The E-Government Act created a federal office responsible for organizing rules and reports from various agencies into a single searchable source.[143] Congress, recognizing the privacy concerns that such a centralized and searchable database raised, included a provision that requires federal agencies to conduct "privacy impact assessments" (PIAs) whenever they buy new technologies.[144] "A PIA is an analysis of how personally identifiable information is collected, used, disseminated, and maintained," and it is intended "to demonstrate that system owners and developers have consciously incorporated privacy protections throughout the entire life cycle of a system."[145]

---

140. Five of the ten most populous metropolitan areas in the country, for instance, include cities in more than one state. U.S. CENSUS BUREAU, U.S. DEP'T OF COMMERCE, CENSUS 2000: RANKING TABLES FOR METROPOLITAN AREAS (PHT-T3) tbl.3 (2001), *available at* http://www.census.gov/population/cen2000/phc-t3/tab03.pdf. A sixth metropolitan area straddles the U.S.-Canadian border. *See* John Wisely, *Security Gets Even Tighter on Border with Canada*, DET. FREE PRESS, Sept. 11, 2007, at 1.

141. Savage, *supra* note 114.

142. Pub. L. No. 107-347, 116 Stat. 2899, codified at 44 U.S.C. § 3501 (Supp. II 2002).

143. White House, About E-Gov: The E-Government Act of 2002, http://www.whitehouse.gov/omb/egov/g-4-act.html (last visited Apr. 4, 2008).

144. Memorandum from Joshua B. Bolten, Director, Office of Mgmt. and Budget to Heads of Executive Departments and Agencies, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (Sept. 26, 2003), *available at* http://www.whitehouse.gov/omb/memoranda/m03-22.html; Privacy Impact Assessment for the SBInet Program; Rebecca Fairley Raney, *In the Next Year, the Federal Government Will Move to Give the Public Easier Online Access to Data Services*, N.Y. TIMES, Dec. 23, 2002, at C4.

145. PRIVACY OFFICE, DEP'T. OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENTS: OFFICIAL GUIDANCE 5 (2007) [hereinafter OFFICIAL GUIDANCE], *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_guidance_may2007.pdf.

The PIA requirement, under the E-Government Act, applies to federal agencies but does not apply to state or local governments.[146] Congress and federal agencies may extend requirements to the states as conditions for accepting federal funding.[147] The DHS has, so far, declined to extend the PIA requirement.[148] If the DHS installs a new video system, it must conduct a PIA.[149] If the DHS distributes grant money to the states and the states use that money to install the same video system, the states do not have to conduct PIAs.[150] This loophole in the PIA requirement allows states to use federal money while ignoring the same privacy interests that the federal government itself must attempt to protect.[151]

A requirement that state and local governments conduct PIAs before deploying video systems could serve as the kind of loose regulation that protects privacy and other policy interests while leaving those governments significant flexibility. In 2007, the DHS conducted a PIA that hints at the way a PIA requirement attached to video system grants might work in practice. The PIA was for a video system that DHS planned to deploy along the Arizona-Mexico border as part of its Secure Border Initiative (SBInet).[152] The SBInet PIA specified how long the system would retain footage, who would have access to it and to camera controls, and what

146. *See* 44 U.S.C. § 3501 sec. 208 (Supp. II 2002).

147. South Dakota v. Dole, 483 U.S. 203, 206 (1987) ("Incident to [the spending power] power, Congress may attach conditions on the receipt of federal funds, and has repeatedly employed the power 'to further broad policy objectives by conditioning receipt of federal moneys upon compliance by the recipient with federal statutory and administrative directives.'").

148. Remarks of Toby M. Levin, Senior Advisor to the Dep't. of Homeland Security Privacy Office, at the U.S. Dep't. of Homeland Security Public Workshop—CCTV: Developing Privacy Best Practices, Panel on Developing Privacy Best Practices for the Use of CCTV 30 (Dec. 17, 2007), http://www.dhs.gov/xlibrary/assets/privacy/privacy_workshop_cctv_Transcript-_Developing_Privacy_Best_Practices_Panel.pdf.

149. The agency must conduct a PIA when "developing or procuring any new technologies or systems that handle or collect personally identifiable information." Personally identifiable information "is any information that permits the identity of an individual to be directly or indirectly referred." OFFICIAL GUIDANCE, *supra* note 145, at 8, 5.

150. Remarks of Deidre K. Mulligan, Director, Samuelson Law, Tech. & Pub. Pol'y Clinic, UC Berkeley School of Law, at the U.S. Dep't. of Homeland Security Public Workshop—CCTV: Developing Privacy Best Practices, Panel on Developing Privacy Best Practices for the Use of CCTV 30 (Dec. 17, 2007), http://www.dhs.gov/xlibrary/assets/privacy/privacy_workshop_cctv_Transcript-_Developing_Privacy_Best_Practices_Panel.pdf.

151. *Id.*

152. DEP'T. OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE SBINET PROGRAM 2 (2007) [hereinafter SBINET PIA], http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_sbinet.pdf.

kind of training those individuals would receive.[153] The PIA provided that internal system checks like passwords and periodic audits would guard against unwanted access or misuse.[154] And it required DHS to create policies and procedures that accounted for privacy interests.[155]

In the end, the PIA process forced DHS to create a set of practical rules that applied to a specific video system. These rules are a form of regulation. They apply to the way users operate a system. In that sense, they are similar to the policies and procedures that local governments have created for more traditional police matters like pursuit and use-of-force. The traditional policies govern the use of a gun or patrol car while the rules the PIA helped to generate govern the use of a video system.

Congress could extend the PIA requirement to state and local governments through legislation that requires state and local governments that spend federal funds on video systems conduct PIAs, or take similar measures that achieve the same results that PIAs would. This legislation could, for instance, require that state and local governments develop written policies and procedures governing the use of video systems. The legislation could further require those policies to address a set of specified issues like who will have access to the system and how long the system will retain video footage. The process of addressing those issues could indirectly force state and local governments to work through PIA-style questions and could, like a PIA, culminate in the creation of ground-level regulation with built-in privacy protections.

C. State Legislation

State legislation could not provide all the benefits that federal legislation could. It could not integrate video surveillance into the existing federal surveillance statutory framework, and it could not articulate the relationship between video surveillance and national security goals. Nor could state legislation set national standards in the way that federal legislation could. However, although not sufficient, state legislation could serve as a substitute or even a supplement for federal legislation.

State-level legislation offers three principal benefits. The first is that video surveillance legislation fits within a state's police power.[156] Califor-

153. *Id.* at 8-12.

154. *See id.* at 10-11.

155. *Id.* at 4.

156. Within the federal system, while the federal government is one of limited powers, the states, as sovereign entities, retain the general police power—the power to regulate public health, safety, morals, and welfare. The Tenth Amendment reserves the police power to the states. U.S. CONST. amend. X. ("The powers not delegated to the United

nia, for one, has already imposed limited regulations on some types of video surveillance. It requires local governments to keep footage for at least a year if the video system that recorded that footage was "designed to record the regular and ongoing operations of the departments . . . including mobile in-car video systems, jail observation and monitoring systems, and building security taping systems."[157] This statute does not apply to the footage collected through the surveillance of public areas like street corners and parks.[158] A similar statute, however, could build upon it and require that police departments retain footage for at least a certain period of time, or for less than a certain period of time. The state could even simply require departments to have stated retention policies.

The second principal benefit is that states distribute grants from the federal government (particularly DHS) to local governments.[159] The states are conduits through which requests and financial grants from the federal government must pass. States could impose an E-Government-style PIA requirement on grant applicants or recipients. Such a requirement would offer the same advantages that a similar federal-level PIA requirement would. The third principal benefit is that state legislation could address the manner in which video surveillance or other new technologies interact with state-level privacy protections.[160]

V. LOCAL REGULATION

Local regulation would generally take the form of a set of written policies and procedures that govern the use of video systems. Some of the cities that have developed video surveillance policies have required their city

States by the Constitution, nor prohibited by it to the states, are reserved to the states respectively, or to the people.").

157. CAL. GOV'T CODE § 34090.6(c) (Supp. 2008).

158. Public video surveillance would be occurring in the locations provided in the statute and would not be intended to monitor the "operations of the departments." *Id.*

159. Remarks of Amy Lassi, Federal Emergency Management Agency Grant Program Directorate, at the U.S. Dep't. of Homeland Security Public Workshop—CCTV: Developing Privacy Best Practices, Community Perspectives Panel 21 (Dec. 17 2007), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_workshop_cctv_-Transcript_Community_Perspectives_Panel.pdf (discussing the process for distributing grants).

160. Several states have constitutional privacy protections that are stronger than their federal-level counterparts. The California and Hawaii provisions are among the most notable. *See* Stephen E. Henderson, *Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information From Unreasonable Search*, 55 CATH. U. L. 373, 428 (2006).

councils to approve them;[161] others have allowed their police departments to adopt policies as internal administrative rules.[162] Existing policies tend to address the same issues that the SBInet PIA addressed. These issues include what the purpose of the system is, how to notify people that cameras are recording them, how to train system operators, and how long to retain video footage.[163]

These written ground-level policies are indispensable. Federal and state regulation will not succeed without local action. It is local governments that intimately understand systems work. It is local governments that know what kinds of policies would work best with those systems. In California, for instance, San Francisco does not have officers watching surveillance feeds in real-time; officers may access footage only after the fact, if investigating a crime.[164] The Central Valley town of Clovis, by contrast, not only requires officers to actively watch video feeds but transmits those feeds to patrol cars so that officers can access them from the field.[165]

Good policies benefit not only privacy interests but also local governments themselves. Policies could help to reduce the odds of misuse and of potential civil liability that might arise from the misuse of video systems.[166] They could help build community support by showing that police

161. *See, e.g.*, S.F., CAL., COMMUNITY SAFETY CAMERA ORDINANCE § 19 (2006); D.C. Metropolitan Police Dep't, CCTV—Policies and Procedures, http://mpdc.dc.gov/mpdc (follow "Programs & Resources" link from left-hand navigation menu; select "Closed Circuit Television (CCTV)" from list of resources; then select "Policies & Procedures" from left-hand navigation menu) (last visited Apr. 4, 2008).

162. City of Clovis, Cal. Police Dep't., Closed Circuit Television System Policy; City of Richmond, Cal. Police Dep't., Use of Closed Circuit Television Cameras: Public Camera Policy and Procedure.

163. *Compare* SBINET PIA, *supra* note 152, *and* City of Santa Monica, Cal. Police Dep't., Public Video Security System Policy (2006). *See also*, City of Stockton Police Dep't., General Order J-1, Closed Circuit Television Cameras (2007); City of Palm Springs Police Dep't., General Order, Downtown Video Surveillance Camera Policy, General Order 2002-05 (2002).

164. S.F., Cal., Community Safety Camera Ordinance § 19 (2006).

165. Law Enforcement Perspectives, *supra* note 46, at 5-6.

166. Police misconduct could lead to constitutional actions, under 42 U.S.C. 1983, and, in some states, tort claims against local governments. 3 ANTIEAU ON LOCAL GOVERNMENT LAW § 38.02 (2d ed. 2007). Both officers and local governments can be held liable for constitutional violations. 42 U.S.C. § 1983 (2000) ("Every person who, under color of [law], subjects, or causes to be subjected, any citizen of the United States or other person within the jurisdiction thereof to the deprivation of any rights, privileges, or immunities secured by the Constitution and laws, shall be liable . . . for redress."). Municipal liability, as opposed to the liability of individual officers, can be found "only where the municipality *itself* causes the constitutional violation at issue . . . 'It is only

intend to use what is sometimes a controversial technology in a responsible way.[167] And they could improve system effectiveness by ensuring that police use the systems in an optimal way and for the stated purpose.

VI. CONCLUSION: TRAINING AND BEST PRACTICES

Legal history is full with examples of laws that failed because individuals ignored them or only nominally followed them.[168] To succeed, laws must shape behavior and become incorporated into custom and habit.[169] Video surveillance regulation is no different. If the police departments do not appreciate the goals of video surveillance regulation, they can probably figure out a way to work around it.[170] But there is reason to believe that the law enforcement community wants to use video systems in a manner that respects privacy rights and that it wants to develop and promote best practices.[171] To make the most of this support, the law enforcement community and privacy activists must work together to develop and push through regulation now. They must act while the video surveillance infrastructure is still being built and can still be designed to incorporate privacy concerns. If they wait, it will be that much harder to try to build privacy protections into a completed surveillance infrastructure.

---

when the 'execution of the government's policy or custom . . . inflicts the injury' that the municipality may be held liable under § 1983.'" City of Canton v. Harris, 489 U.S. 378, 385 (1989). A written CCTV policy can help prevent misuse. CONSTITUTION PROJECT, *supra* note 11, at xii. And while the existence of a policy could not, on its own, prove a particular custom, it could serve as evidence of one. St. Louis v. Praprotnik, 485 U.S. 112, 127 (1988).

167. Ken Hampian, *How to Cure (or at Least Treat) the Video Monitoring Heebie Jeebies*, PUB. MGMT., Apr. 2007, at 25.

168. Thomas B. Stoddard, *Bleeding Heart: Reflections on Using the Law to Make Social Change*, 72 N.Y.U. L. REV. 967 (1997).

169. *Id.*

170. W. Dwayne Orrick, *Developing a Police Department Policy-Procedure Manual*, BIG IDEAS FOR SMALLER POLICE DEPARTMENTS (Int'l Ass'n of Chiefs of Police, Alexandria, Va.) at 11 (Winter 2005) (explaining that "the custom is policy . . . Informal customs attack the credibility of the department's operational procedures and administration"). There is also an abundance of literature regarding the failure of the warnings the Court established in *Miranda v. Arizona*, 384 U.S. 436 (1966), to adequately protect suspects from coercive police practices. Richard A. Leo, *Miranda's Revenge: Police Interrogation as a Confidence Game*, 30 LAW & SOC'Y REV. 259 (1996); Richard A. Leo & Welsh S. White, *Adapting to Miranda: Modern Interrogators' Strategies for Dealing with the Obstacles Posed by Miranda*, 84 MINN. L. REV. 397 (1999).

171. Law Enforcement Perspectives, *supra* note 46, at 14.