Article

Surveillance, Policing, and Democracy

Deirdre K. Mulligan[†] **and Stephen B. Wicker**[††]

Law enforcement has a long history of using sensing devices to assist in investigations. Such devices range from dogs and search lights, to microphones[1] or bugs worn by informants and undercover officers, to night vision goggles, infrared imaging devices,[2] spectrometers, and chromatographers.[3] Some sensing

† Assistant Professor, School of Information, University of California at Berkeley.

†† Professor, School of Electrical and Computer Engineering, Cornell University. Much appreciation to Jennifer King, Pamela Samuelson, Jennifer M. Urban, Kenneth Bamberger, Fred Cate, and the participants in the *Un-Blinking: New Perspectives on Visual Privacy in the 21st Century* Symposium, and the *Privacy in Public: Ethics, Privacy and the Technology of Public Surveillance* workshop at the Poynter Center for the Study of Ethics and American Institutions at the University of Indiana at Bloomington, as well as the TRUST (Team for Research in Ubiquitous Secure Technology) Advisory Board for their insights, comments, and discussion. Thanks to Jennifer King and Stephen Rafael for their collaboration on the San Francisco Community Safety Camera Study. Thanks to David Culler, Joseph Hellerstein, and David Wagner for multiple cross-disciplinary conversations about the privacy issues in sensor networks. Thanks to Will DeVries, Nicole Ozer, and Sharon Bradford Franklin for numerous conversations about the implications of video surveillance. Thanks to David Snyder, Larisa K. Mann, Jeremy Brown, Sameer Pai, Marci Meingast, Tara Wheatland, Becky Hurwitz, Mikhail Lisovich, and David C. Yang for research support and collaboration on related projects. Thanks to Nicole M. Murphy, Symposium Articles Editor at the University of Minnesota Law School for expert editing and abundant patience. Support for this work was provided by TRUST which receives support from the National Science Foundation (NSF award number CCF-0424422).

1. *See, e.g.*, Kee v. City of Rowlett, 247 F.3d 206, 208–09 (5th Cir. 2001) (finding the public was unwilling to recognize an expectation of privacy in words spoken at a public grave as reasonable, absent some showing that the plaintiffs expected their words not to be overheard, and allowing police to plant a microphone at a public gravesite during a public memorial service).

2. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 27 (2001) (disallowing the use of a thermal imaging device to detect marijuana plants in a house because the defendant reasonably assumed his actions within his home would remain private); United States v. Coplen, 541 F.2d 211, 213 (9th Cir. 1976)

devices enhance existing senses while others extend the capacity of humans to sense physical phenomena.[4] Historically, sensing devices have been used predominantly in the context of a specific investigation.[5] With the proliferation of permanently installed video surveillance systems, and the use of other sensing devices to monitor public places for health and safety reasons, we face a future of suspicionless surveillance and data collection.[6] While a variety of sensors—for example, gunshot sensors and spectrometers—are being deployed in select settings,[7] the largest growth in sensing technology aimed at the general public is video surveillance.[8] The Department of Homeland Security (DHS) has provided millions of dollars worth of grant monies to states and localities to purchase and up-

(discussing governmental use of infrared equipment to observe a narcotics smuggling operation at night); United States v. Porco, 842 F. Supp. 1393, 1395–96 (D. Wyo. 1994), *aff'd*, United States v. Cusumano, 83 F.3d 1247 (10th Cir. 1996) (discussing use of thermal imaging equipment as a means of surveillance).

3. *E.g.*, Peter Joseph Bober, *The "Chemical Signature" of the Fourth Amendment: Gas Chromatography/ Mass Spectrometry and the War on Drugs*, 8 SETON HALL CONST. L.J. 75, 78–79 (1997) (discussing the background of gas chromatography). Like the canine nose, these technologies (chromatography or mass spectrometry), which go by the trade names Sentor and Ionscan (among others), can identify the presence of substances on (or in) luggage and containers without the need to open those containers. *See id.* at 76–77 & n.276. Gas chromatography uses a highly sensitive filtering machine to break down gas samples or liquid mixtures into their molecular subcomponents. *Id.* at 79. The sample is forced through a glass tube filled with special filtration material. *Id.* A detector attached at the outgoing end of the tube records the quantity and concentration of individual molecular compounds. *Id.* A police officer can use an eight-pound sampling unit, which resembles a large flashlight and works like a vacuum, to suck in vapors and particles from the immediate vicinity of a suspected container or individual. *See id.* at 81 & n.39. The analytical unit, also at the scene, then takes this sample and produces a chemical sketch of it, which is then compared to the make-up of known explosives, drugs, etc. *See id.* at 77 & n.15. The assumption is that a positive report establishes the presence of explosives or drugs. *See, e.g.*, *id.* at 110.

4. *See, e.g.*, *id.* at 75–76 (describing American officials' unsuccessful initial search in an attempt to connect a defendant with narcotics, and subsequent success in detecting traces of narcotics with the use of enhanced technology).

5. *See, e.g.*, *Kyllo*, 533 U.S. at 27 (recounting agent responses to suspicious activity by using sensing device to scan petitioner's dwelling).

6. *See* Quentin Burrows, *Scowl Because You're on Candid Camera*, 31 VAL. U. L. REV. 1079, 1079–81 (1997).

7. *See, e.g.*, Bober, *supra* note 3, at 81–82 (discussing the use of a specific high-tech device, known as an "EGIS," used to detect explosives).

8. *See, e.g.*, Burrows, *supra* note 6, at 1079–80 (1997) (discussing the prevalence of video surveillance).

grade video surveillance systems.[9] It is clear from news reports and DHS budget figures that this number continues to rise.[10] Surveillance cameras appear to have no preferred geography; they can be found in large urban areas like New York, Chicago, and Los Angeles, but they also proliferate in rural areas.[11] Dillingham, Alaska (population 2400) has at least sixty police surveillance cameras—three times the number of police surveillance cameras as the District of Columbia—purchased entirely with DHS grant money.[12] Seven surveillance cameras give authorities a panoramic view of the entire town center.[13] Rural Bellows Falls, Vermont (population 3000), more than one hundred miles from any major urban area, has sixteen police cameras monitoring the town center, again courtesy of DHS.[14] Clovis, California, a relatively small town outside Fresno, has an extensive, state of the art video surveillance network—in large part due to the presence of Pelco, a major purveyor of surveillance cameras.[15] Until relatively recently, the town and its police department, like many others, had no official policy about

9. Audrey Hudson, *Counterterror Grants Fund City Cameras, Data Mining*, WASH. TIMES, May 19, 2005, at A03 (quoting DHS spokesman Marc Short who stated that "[i]n 2004, homeland security funds bought $193 million worth of surveillance cameras"); Charlie Savage, *US Doles Out Millions for Street Cameras: Local Efforts Raise Privacy Alarms*, BOSTON GLOBE, Aug. 12, 2007, at A1, *available at* http://www.boston.com/news/nation/washington/articles/2007/08/12/us_doles_out_millions_for_street_cameras/?page=2.

10. *See* Savage, *supra* note 9.

11. *See* John Buntin, *Long Lens of the Law*, GOVERNING, May 2009, at 24 (discussing 480 cameras in Baltimore, MD, $4 million spent on cameras and license plate readers in Pittsburgh, PA, $3 million to double the existing sixty-eight camera system in Buffalo, NY, and nearly doubling the fifty-four camera network in Indianapolis, IN); David A. Fahrenthold, *Federal Grants Bring Surveillance Cameras to Small Towns: Village in Vermont Has Almost as Many as D.C.*, WASH. POST, Jan. 19, 2006, at A1; Nicole Radzievich, *Security Cameras May Be Required: Bethlehem Weighs Plan for Outside Surveillance on Businesses in City*, MORNING CALL (Allentown, PA), Oct. 30, 2007, *available at* http://articles.mcall.com/2007-10-30/news/3796569_1_security-cameras-parking-lot-business (reporting that in 2001, Wilmington, Deleware was the first city to videotape the entire downtown area).

12. *Compare* Tomas Alex Tizon, *80 Eyes on 2,400 People*, L.A. TIMES, Mar. 28, 2006, at A1 (discussing the surveillance cameras in Dillingham), *with* Fahrenthold, *supra* note 11 (noting the District of Columbia has around nineteen surveillance cameras).

13. *See* Tizon, *supra* note 12.

14. *See* Fahrenthold, *supra* note 11.

15. *See* Demian Bulwa, *Future Fuzzy for Government Use of Public Surveillance Cameras*, S.F. CHRON., July 23, 2006, at A1 (reporting that Pelco, "the world's largest supplier of the cameras," is the biggest employer in Clovis and "uses Clovis as a showpiece and a laboratory").

how the system or the video footage it creates were to be used.[16] The same story is playing out from coast to coast, usually with significant help from DHS grants.[17] Towns like Ridgely, Maryland and Galax, Virginia, along with cities like New York and Chicago, have rushed to equip their town centers—their public places—with state-of-the-art surveillance technology.[18]

The next wave in video surveillance systems—the combination of private and public surveillance systems to create a seamless surveillance "blanket" over broad swaths of the public sphere—is underway.[19] In places like Fresno, California officials plan to merge the city's public and private surveillance systems, allowing police and police dispatchers to view private security cameras through the Internet.[20] Other cities are requiring stores to not only install video surveillance systems aimed at parking lots and other outdoor spaces as a condition of doing business, but also to provide the police with a live feed of the video images and the ability to control the system.[21] Other jurisdictions are attempting to integrate public and private cameras—including those inside business establishments—into a seamless surveillance network accessible from police cruisers as well as other access points.[22]

The hundreds of millions of dollars allocated by DHS as well as funds from drug forfeitures and other state and local police funds reduce the oversight local communities have over the deployment of permanent public video surveillance systems.[23] The normal political deliberation and up-front oversight of these systems that would occur during budgeting is largely side-stepped because there is no need for appropriations from

16. *See id.*; Fahrenthold, *supra* note 11 (noting that some cities have policies implemented for video surveillance, while others do not).

17. *See* ELEC. PRIVACY INFO. CTR., SPOTLIGHT ON SURVEILLANCE: MORE CITIES DEPLOY CAMERA SURVEILLANCE SYSTEMS WITH FEDERAL GRANT MONEY (2005), http://www.epic.org/privacy/surveillance/spotlight/0505/ (last visited Mar. 11, 2010) [hereinafter SPOTLIGHT ON SURVEILLANCE].

18. *See* Bulwa, *supra* note 15; Fahrenthold, *supra* note 11.

19. *See* Denny Boyles, *ACLU Irked by Fresno Police Proposal to Double Cameras*, FRESNO BEE, Mar. 22, 2006, at A1; Bulwa, *supra* note 15 (discussing Clovis' outfitting of police cars with viewing screens, wireless cameras, and automatic license plate recognition technology).

20. *See* Boyles, *supra* note 19.

21. *See* Bulwa, *supra* note 15; Radzievich, *supra* note 11.

22. *See* Boyles, *supra* note 19.

23. *Cf.* Tizon, *supra* note 12 (discussing the use of Homeland Security funds to purchase extensive surveillance systems in Dillingham, Alaska, much to the opposition of local citizens).

the state or local government when the systems are funded directly by the DHS.[24] Cities around the country have erected elaborate state-of-the-art surveillance systems, often with little oversight or public input.[25] There is little indication that municipalities that have installed, or plan to install, video surveillance systems are making any effort to notify the public of such plans.[26] For example, the U.S. Park Police in Washington, D.C. installed sophisticated surveillance cameras on the National Mall without notifying the public, while the city's police department installed nineteen cameras in commercial districts and other tourist hot spots,also without public notice.[27] Public discussion and debate about the deployment of such systems is the exception, not the norm.[28]

Given that many of the permanent public video surveillance systems circumvent the public review that occurs during the budgeting process, it is perhaps not surprising that the majority of them come into existence without laws or even guidelines to control their use. A 2001 survey conducted by the International Association of Chiefs of Police of more than 200 law enforcement agencies found that fifty-four percent of responding agencies provided no formal training in how to use closed-circuit television (CCTV) systems.[29] While they are often put forward to reduce crime, few towns or cities have enacted procedures to measure their effectiveness.[30] For example, the

24. *Cf.* Bulwa, *supra* note 15 (noting that surveillance systems, often funded with DHS grants, are being implemented almost too swiftly and without much oversight); Savage, *supra* note 9 (describing various DHS funding efforts, and noting the difficulty in tracking how funds are spent).

25. *See* MARK SCHLOSBERG & NICOLE A. OZER, ACLU, UNDER THE WATCHFUL EYE: THE PROLIFERATION OF VIDEO SURVEILLANCE SYSTEMS IN CALIFORNIA 2 (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.

26. *See, e.g.*, Electronic Privacy Information Center, EPIC Alert, July 22, 2003, http://epic.org/alert/EPIC_Alert_10.15.html (last visited Mar. 11, 2010).

27. *See id.*; *see also* Fahrenthold, *supra* note 11.

28. *See, e.g.*, SCHLOSBERG & OZER, *supra* note 25, at 2. ("Cities throughout California have approved and implemented camera systems without guidelines to guard against abuse and, in most circumstances, with little or no public debate.").

29. LAURA J. NICHOLS, INT'L ASS'N OF CHIEFS OF POLICE, CUTTING EDGE OF TECHNOLOGY: THE USE OF CCTV/VIDEO CAMERAS IN LAW ENFORCEMENT 2, 7 fig.4 (2001), *available at* http://www.theiacp.org/LinkClick.aspx?fileticket=Ck%2B1Lk%2BxNbE%3D&tabid=87.

30. *See id.* at 5; SCHLOSBERG & OZER, *supra* note 25, at 2, 16 (noting that no California jurisdiction has conducted a comprehensive evaluation of the cameras' effectiveness, and few towns are making any effort whatsoever to

above report found that ninety-six percent of responding agencies had no way of evaluating whether surveillance systems helped reduce crime.[31]

Two notable exceptions are the District of Columbia and San Francisco. Police in the District of Columbia have agreed to use the cameras only during mass demonstrations and civic emergencies,[32] and not to arbitrarily monitor anyone because of race or gender.[34] The District of Columbia's city council passed regulations calling for the cameras to be used only to monitor traffic, large demonstrations, and city emergencies.[35] The regulations also mandate that the cameras be installed only in public spaces where people would have a reasonable expectation of being videotaped, and they prohibit police from using the devices to watch for ordinary street crime.[36] The police are also required to give community updates about the surveillance system, and to perform routine audits of the police department's use of system.[37] The police chief must also provide public notice of the police department's intention to install any new cameras, and the public notice must include the CCTV system's general capabilities and viewing area, though it does not have to mention the precise location of a new camera.[38] The regulations also require a thirty-day public comment period.[39] These strictures apply only to the city's police department, not the federally-run cameras on the National Mall.[40]

The San Francisco Board of Supervisors enacted a City Ordinance ("CSC Ordinance")[41] governing the Community Safety Camera program comprised of seventy-one cameras connected to a base station.[42] The aims of the CSC Ordinance are "to regu-

evaluate effectiveness).

31. *See* NICHOLS, *supra* note 29, at 5.

32. *See* 24 D.C. Reg. 938 (Feb. 2, 2007).

34. Fahrenthold, *supra* note 11.

35. *See* 24 D.C. Reg. 938.

36. *Id.*; Eric M. Weiss, *D.C. Considering More Police Cameras: London Bombings Prompt New Debate on Surveillance of Public Places*, WASH. POST, July 14, 2005, at B1.

37. 24 D.C. Reg. 938.

38. *Id.*

39. *Id.*

40. *Cf. id.* (discussing applications of the regulations).

41. San Francisco, Cal., Ordinance 127-06 (June 7, 2006) (codified at 19 S.F., CAL., ADMIN. CODE §§ 1–8 (2006)), *available at* http://www.sfbos.org/ftp/uploadedfiles/bdsupvrs/ordinances06/o0127-06.pdf. Supervisor Mirkarimi led its passage. *See id.*

42. *Cf. id.* (detailing the definitions and requirements of the ordinance).

late the installation of community safety cameras, prescribe a notification and approval process for the installation of cameras, and establish protocols for oversight and access to video recordings.'"[43] The CSC Ordinance is the most comprehensive and enforceable framework covering a video surveillance system used by police in the country.[44]

Fueled by fears of terrorism, a "keeping up with the Jonese's" mentality,[45] and the availability of federal money to secure infrastructure, video surveillance systems appear destined to proliferate across the United States.[48] At this point, similar to the United Kingdom, the United States seems poised to sleep walk into a public environment sporting 24/7 surveillance with little evaluation of its utility to police or its impact on the relationship between policing and democracy.[49] The first U.K. study of CCTV systems occurred in 2005,[50] some forty-five years after the first state-sponsored cameras were installed and after mil-

The seventy-one cameras currently deployed by the City consist of three types of cameras—fixed-position network cameras that cannot be manipulated through software (and therefore cannot be controlled remotely); pan-tilt-zoom (PTZ) cameras which can be remotely repositioned and focused remotely through software; and nonmechanical, fixed-position, mini-dome network cameras (fish-eye lens cameras) which have a 360º field of view—with resolutions ranging between two and five megapixels (MP). JENNIFER KING, DEIRDRE K. MULLIGAN & STEVEN RAPHAEL, CENTER FOR INFO. TECH. RESEARCH IN THE INTEREST OF SOC'Y, CITRIS REPORT: THE SAN FRANCISCO COMMUNITY SAFETY CAMERA PROGRAM 170–71 (2008), *available at* http://www.citris-uc.org/files/CITRIS%20SF%20CSC%20Study%20Final%20Dec%202008.pdf [hereinafter CITRIS REPORT]. The cameras are all networked and connected to a base station server in a wired or wireless fashion. *Id*.

43. San Francisco, Cal., Ordinance 127-06 (June 7, 2006).

44. *See* CITRIS REPORT, *supra* note 42, at 9–10.

45. *See, e.g.*, Public Workshop CCTV: Developing Privacy Best Practices, Remarks at the Department of Homeland Security Privacy Office (Dec. 17, 2007) (transcript available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_workshop_cctv_Transcript_Community_Perspectives_Panel.pdf) (discussing the methods used by various community leaders to implement local surveillance systems, and noting the race amongst local officials for increased surveillance capabilities with a fully supportive community).

48. *See* SPOTLIGHT ON SURVEILLANCE, *supra* note 17. Although this Article is about state-run systems, it is notable that today, surveillance in public places is just as likely to be the activity of a single individual as it is the government.

49. *Cf.* Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213, 219–23 (2002) (comparing surveillance in the United States with surveillance in the United Kingdom).

50. *See* MARTIN GILL & ANGELA SPRIGGS, HOME OFFICE RESEARCH, HOME OFFICE RESEARCH STUDY 292: ASSESSING THE IMPACT OF CCTV, at i (2005), *available at* http://www.homeoffice.gov.uk/rds/pdfs05/hors292.pdf.

lions of pounds were spent on such systems.[51] The results of the study suggest very limited utility given the size of the investment with no statistically significant impact on crime.[52] In the United States, the cities of Philadelphia, Los Angeles, and, most recently, San Francisco, have studied the efficacy of certain camera installations[53]—none with promising results for violent crime.[55] Most jurisdictions have installed surveillance systems with little knowledge of the academic research documenting their very limited effectiveness in addressing violent crime,[56] little discussion of alternative policing strategies or technology investments, little public input or oversight, and remarkably few policies governing their use.[57]

51. *Cf.* Dep't of Homeland Sec. Data Privacy & Integrity Advisory Comm., Meeting Minutes 29, 31, July 7, 2006 (statement of Clive Norris, Sheffield Univ. Ctr. for Criminological Research), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_06-2006_mtgminutes_AM.pdf [hereinafter Norris Statement] (noting that "CCTV really enters the landscape in the 1960s" and estimating that of the 250 million pounds spent on open-street CCTV, "85 million [came] from the Conservative administration until 1996 and then another 167 million from the Labour administration").

52. *See* GILL & SPRIGGS, *supra* note 50, at 19–31, 120, 145.

53. *See* CITRIS REPORT, *supra* note 42, at 158 ("As of summer 2008, there are only two independent evaluations of surveillance camera programs in the United States: an evaluation of Philadelphia's CCTV camera system . . . and an evaluation of two of Los Angeles's camera installations.").

55. *See id.* ("A review of the academic research conducted over the past fifteen years demonstrates a 'consistent inconsistency': after nearly two decades, there is no definitive answer as to whether or not video surveillance of public places 'works.'"); *see also* AUNDREIA CAMERON ET AL., CAL. RESEARCH BUREAU, MEASURING THE EFFECTS OF VIDEO SURVEILLANCE ON CRIME IN LOS ANGELES 53 (2008), *available at* http://www.library.ca.gov/crb/08/08-007.pdf#search=measuring%20the%20effects%20of%20video%20surveillance%20on%20crime%20in%20los%20angeles&view=FitH&pagemode=none.

56. *See, e.g.*, CAMERON ET AL., *supra* note 55, at 29–53 (discussing the research, statistical findings, and implications of surveillance programs); CITRIS REPORT, *supra* note 42, at 43–90 (empirical evaluation of the surveillance interventions in San Francisco); GILL & SPRIGGS, *supra* note 50, at 19–36 (research study evaluating thirteen CCTV programs and finding only one site with a statistically significant reduction in crime relative to the control area); Leon Hempel & Eric Töpfer, *CCTV In Europe: Final Report* (Urbaneye Project, Working Paper No. 15, 2004), *available at* http://www.urbaneye.net/results/ue_wp15.pdf (discussing the effects of CCTV in Europe).

57. *Cf.* SCHLOSBERG & OZER, *supra* note 25, at 1–18 (discussing various concerns, including limited effectiveness and regulation, relating to video surveillance systems). Although very few jurisdictions have formal regulation of CCTV, where it is regulated, regulations are often of a subset of the CCTV systems that operate in the jurisdiction because of the piecemeal and fragmented approach to funding, installation, and use. *Cf.* Buntin, *supra* note 11, at 26 (discussing use of a significant portion of DHS funds sent to state and local governments for camera purchase and use of DHS and asset-forfeiture

This Article suggests that permanent public video surveillance systems should be constrained not because of controversial expectations of privacy but instead based on democratic theory, developments in criminal procedure, and approaches to managing institutions of policing. Specifically, Parts I and II argue that the current framework focusing on balancing the privacy interests of individuals against the needs of law enforcement discounts the problematic features of surreptitious surveillance for traditional democratic controls on policing, which aim to protect not only individuals but the balance between policing and openness in free societies. Parts III and IV consider the role that bedrock principles of criminal procedure including transparency, limits on police discretion and oversight should play in structuring police use of video surveillance systems, and sensing technology more generally. Part IV specifically provides some technical and policy recommendations to guide efforts to regulate sensing technology.

I. TRADITIONAL OBJECTIONS TO VIDEO SURVEILLANCE SYSTEMS

Critics of permanent public video surveillance systems (PPVSS) portray them as a bellwether technology signaling a move toward a totalitarian government and a conformist society.[58] Standard objections to pervasive video surveillance in public places include invasion of privacy,[59] the concomitant reduc-

funds to build the Baltimore camera network); James Hohmann, *Metro Will Equip Buses, Trains with Cameras: Surveillance Meant To Manage Crowds and Deter Crime*, WASH. POST, Sept. 29, 2009, at B4 (discussing Metro accepting $27.8 million in DHS grants to pay for video cameras and noting the flood of government money accelerating proliferation of surveillance systems). Communities may have CCTV systems run by police, multiple transit authorities, and housing authorities among others. *Cf.* CITRIS REPORT, *supra* note 42, at 122–36 (discussing the management of San Francisco's camera program).

58. For example, see SCHLOSBERG & OZER, *supra* note 25, at 3 (discussing parallels between George Orwell's novel, *1984* and the spread of government use of video surveillance today).

59. *See id.* Many theories of privacy including the right to limit access to the self, the right to be forgotten, and the right to control information about the self have been used to argue against permanent public video surveillance in public places. *Cf. id.* at 6–10 (discussing various privacy rights). Examined closely these theories seek to protect different objects (information, the self in some inchoate sense, the recording of the physical self) and rely on different justifications (autonomy, self-development, a moral sense of personal wholeness). *Cf. id.* (discussing legal bases of privacy rights).

tion in anonymity, the chilling effect on freedom of association and expression, the related impact on use of public places, potential discrimination, and voyeurism.[60]

Critics of permanent public video surveillance systems are concerned with several forms of privacy intrusions.[61] In public places, PPVSS change the economics of policing—in the words of one scholar it removes a "structural barrier"[62] that has practically afforded privacy protection—magnifying surveillance capacity. In the words of one critic, the PPVSS are "[m]ass surveillance . . . directed toward everyone . . . ."[63] A related but distinct criticism is the ease with which the state can amass information on individuals who have done nothing wrong.[64] Cameras that pan, tilt, zoom, and alter what is visible (infrared) do not merely replace an officer on the street.[65] Critics as-

60. *See, e.g.*, *id.* at 1–18.

61. *See, e.g.*, *id.* at 7–9. Scholars have examined the privacy implications of a wide range of surveillance and dataveillance technologies and reliance on networks generally. *See generally, e.g.*, DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE (2004); Anita L. Allen, *Dredging Up the Past: Lifelogging, Memory, and Surveillance*, 75 U. CHI. L. REV. 47, 55–70 (2008) (discussing privacy and other implications of lifelogging (sensory documentation by individuals)); Julie E. Cohen, *Cyberspace as/ and Space*, 107 COLUM. L. REV. 210 (2007) [hereinafter *Cyberspace*]; Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373 (2000); A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461 (2000); Benjamin J. Goold, *Surveillance and the Political Value of Privacy*, 1 AMSTERDAM L.F. 3 (2009) (discussing political value of privacy in a free society); Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193 (1998); Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801 (2004); Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?*, 44 FED. COMM. L.J. 195 (1992); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609 (1999); Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083 (2002).

62. *Cf.* Harry Surden, *Structural Rights in Privacy*, 60 SMU L. REV. 1605 (2007) (discussing the relationship between structural barriers, which include explicit and implicit constraints on behavior, and their impact on personal privacy).

63. Jeremy Redmon, *Atlanta Seeks to Add 500 Surveillance Cameras*, ATLANTA J.-CONST., Oct. 24, 2009, *available at* http://www.ajc.com/news/atlanta/atlanta-seeks-to-add-171808.html (quoting Marc Rotenberg, executive director of the Electronic Privacy Information Center).

64. *See* SCHLOSBERG & OZER, *supra* note 25, at 4 (government surveillance monitoring "gives the government a vast quantity of information on private citizens that would otherwise be unavailable, allowing it to monitor people engaging in wholly innocent and constitutionally protected behavior").

65. *See* THE CONSTITUTION PROJECT, GUIDELINES FOR PUBLIC VIDEO SURVEILLANCE: A GUIDE TO PROTECTING COMMUNITIES AND PRESERVING CIV-

sert that "words on a vial of prescription drugs, the moving lips of a couple engaged in hushed conversation, or diary entries written by a person sitting on a park bench" may be accessible to the state using PPVSS although the individual has no intention to "expose"[66] them to the public. Activities that occur in public, but are practically private[67] against the natural sensing capacity of humans, are now treated as if they were available to law enforcement physically policing the public place. Individuals are stripped of the clues they need to manage their exposure and privacy in public places. Here the privacy loss stems not from the watching but primarily from the aggregation of images over time and across spaces that can be used to create detailed dossiers on individuals' whereabouts, associations, and habits. "Everyone gets swept into these big databases."[68]

Concern about the "chilling effect" on individuals' use of public places, particularly "expressive" places, is raised in opposition to video surveillance. Concerns about the creation of "container"[69] space, the squelching of spontaneous social behavior,[70] interference with peaceful political protests, and fracturing of the lively public sphere essential to democratic discourse are also raised.[72] Although little empirical research has been undertaken to study whether public video surveillance systems chill the speech or associational activities of individuals, theoretical research from various disciplines support such a conclu-

IL LIBERTIES 2 (2007), *available at* http://www.constitutionproject.org/pdf/Video_Surveillance_Guidelines_Report_w_Model_Legislation4.pdf.

66. *Id*. at 8. In *Katz v. United States*, the court wrote, "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection," 389 U.S. 347, 351 (1967). However, it found that a conversation taking place in a public phone booth was nonetheless protected—it was not exposed. *See id*. at 347, 359.

67. *See* SCHLOSBERG & OZER, *supra* note 25, at 4. A similar issue occurred with the move to make court records remotely accessible, thus making something that was legally accessible but practically not utilized increasingly accessible. *Cf. id*. (noting that cameras can zoom in on the title of a book, which was not previously possible). Surveillance systems, however, go beyond making what is legally possible more practical, and actually extend the scope of what is legally open for viewing. *Cf. id*. at 3 (arguing that the government's expanding surveillance capabilities threaten privacy rights).

68. Redmon, *supra* note 63.

69. *See* Hille Koskela, *The Gaze Without Eyes': Video-Surveillance and the Changing Nature of Urban Space*, 24 PROGRESS IN HUM. GEOGRAPHY 243, 248–51 (2000), *available at* http://www.geog.psu.edu/courses/geog497b/Readings/Koskela.pdf.

70. *Id*. at 247.

72. *See* SCHLOSBERG & OZER, *supra* note 25, at 10; THE CONSTITUTION PROJECT, *supra* note 65, at 9.

sion,[74] as does the deterrent theory on which many public video surveillance installations rest.[75] Advocates and scholars have pointed out that the rise of video surveillance in public places increases the capacity of the government to tie individuals to expressive and associational activities.[76] As surveillance systems become more sophisticated, the ability of government agents to monitor and track individuals and activities revealing political affiliations, social connections, and even shopping habits increases greatly.[77] Opponents argue the increased ability of government to secretly monitor will cause individuals to self-censor in public places.[78] As history has shown, systems of state surveillance have been abused to squelch dissent and interfere with legitimate political movements.[79]

74. *Cf.* David Murakami Wood & Stephen Graham, *Permeable Boundaries in the Software-Sorted Society: Surveillance and Differentiation of Mobility*, *in* MOBILE TECHNOLOGIES OF THE CITY 177 (Mimi Sheller & John Urry eds., 2006) (discussing surveillance technology from a philosophical perspective); Kevin D. Haggerty & Richard V. Ericson, *The Surveillant Assemblage*, 51 BRITISH J. SOC. 605, 622 (2000) (discussing various theories of surveillance and concluding that modern surveillance systems create an "assemblage").

75. *Cf.* THE CONSTITUTION PROJECT, *supra* note 65, at 36 (noting that surveillance systems may deter speech and political activity). Many surveillance systems are installed to deter crime. SCHLOSBERG & OZER, *supra* note 25, at 11. In particular, systems are set up with highly visible cameras, or notice of surveillance, but limited monitoring. *Cf. id.* at 2 (noting that only eighteen cities employ active monitoring). The thought is that criminals will act rationally and not engage in crimes because the cameras elevate the possibility of being caught. *Cf. id.* at 11 (noting that criminals are thought to be deterred by the presence of video surveillance). The assumption that criminals are rational actors does not uniformly bear out in research on the impact of video surveillance systems. *See id.* In some instances there is evidence that property crime is reduced or displaced, but violent crime rates do not appear to be effected by the introduction of public surveillance systems. *See, e.g.*, CAMERON ET AL., *supra* note 55, at 8–9 & fig.1.

76. *See* Marc Jonathan Blitz, *Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World that Tracks Image and Identity*, 82 TEX. L. REV. 1349, 1352–55 (2004); Christopher Slobogin, *supra* note 49, at 219–21, 257–58.

77. *Cf.* Carolyn Y. Johnson, *Project 'Gaydar': At MIT, an Experiment Identifies Which Students are Gay, Raising New Questions About Online Privacy*, BOSTON SUNDAY GLOBE, Sept. 20, 2009, at K1 (discussing how online social networking tools can be used to track and predict characteristics of individual users).

78. *See* SCHLOSBERG & OZER, *supra* note 25, at 6; Blitz, *supra* note 76, at 1352, 1377; Slogobin, *supra* note 49, at 242–47.

79. *See* Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 12 (2004) (noting that instances of governmental misuse of surveillance practices, such as Watergate, are numerous); *cf.* Slobogin, *supra* note 49, at 247–67 (discussing the government's use of surveillance and constitutional implications of public camera surveillance).

Opponents raise concerns that PPVSS may be used to target certain individuals or populations for scrutiny.[80] The locations in which PPVSS are installed will implicate who is subject to scrutiny.[81] In monitored systems the basis upon which individuals are singled out for scrutiny—whether by other individuals or by algorithms—provides an opportunity to introduce bias.[82] Researchers claim that the stratification enabled by the growing stockpiles of data and the knowledge structures that are both derived from and imposed upon people fracture society along various lines that undermine the workings of the public sphere.[83] Researchers have documented the use of video surveillance systems to "clean up" shopping areas and malls by removing individuals viewed as undesirable or deviant.[84] The images from the PPVSS may, as Bentham envisioned, be used to enhance individuals' conformance with social norms (and laws) bringing or keeping them within society's embrace, or they can be used to regulate the flow of people into public places privileging some and excluding others depending on the captured images.[85]

Video surveillance system opponents claim that the ability to invisibly gaze creates unique opportunities for misuse. Stories of such misuse give credence to their concern. In spring 2004, surveillance cameras placed in a Bronx housing project

80. *See, e.g.*, SPOTLIGHT ON SURVEILLANCE, *supra* note 17 (discussing studies showing disproportionate scrutiny of black males); *see also* Hille Koskela, *Video Surveillance, Gender, and the Safety of Public Urban Space: "Peeping Tom" Goes High Tech?*, 23 URB. GEOGRAPHY 257, 263 (2002) (discussing gender imbalance in who is watched and who does the watching).

81. *Cf.* Koskela, *supra* note 80, at 263 (arguing that "surveillance is gendered" because women tend to use public transportation and do the bulk of the shopping in downtown areas where surveillance is prevalent, whereas "most of the persons 'behind' the camera are men").

82. Michael R. Curry, *The Profiler's Question and the Treacherous Traveler: Narratives of Belonging in Commercial Aviation*, 1 SURVEILLANCE & SOC'Y J. 475, 475 (2003) ("[F]ar from being merely expository devices, such narratives are central to the profile's analytical structure; as a consequence, while their promoters laud the profiling systems as neutral analytical devices, embedded within them is a sorting system that might more accurately be described as encoding."). *See generally* Lucas D. Introna & David Wood, *Picturing Algorithmic Surveillance: The Politics of Facial Recognition Systems*, 2 SURVEILLANCE & SOC'Y J. 177, 186 (2004) (discussing the bias embedded in algorithms used for facial recognition systems).

83. Wood & Graham, *supra* note 74, at 188 (discussing implications of software sorting on the public sphere).

84. *See* Koskela, *supra* note 69, at 246 (discussing numerous studies on this phenomenon).

85. *See infra* note 121 and accompanying text.

lobby by the New York City police department captured a man committing suicide by shooting himself in the head.[86] Footage of the twenty-two year old man's death ended up on the internet, where it was visible to millions.[87] The video apparently ended up on the web after a police officer emailed the footage to a friend, setting off a chain of emails that ended with the posting to a website.[88] In a less morbid controversy, a University of Nevada at Reno professor claimed he was being monitored as a whistleblower after officials installed a hidden camera outside his office; university officials claimed the camera was installed for the professor's safety because of recent slurs directed at him.[89] A New York City resident filed a formal complaint with the city's police department after officers observed and recorded nearly four minutes of intimate, amorous activity on the terrace of his Second Avenue penthouse at night.[91] Officers in that instance used a $9.8 million helicopter with thermal imaging equipment and cameras powerful enough to read a license plate from 1000 feet away.[92] Researchers further argue that video surveillance presents particular issues for women in part because the watchers are predominantly men while women are more frequently present in the areas under surveillance.[94]

II. LIMITATIONS OF THE TRADITIONAL CRITIQUES

Despite the force with which video surveillance opponents raise privacy and freedom of expression and association objections, to date these arguments have had little traction in the courts, with legislators, or with the public. Courts have consistently rejected privacy claims against sensory-enhanced government visual observation in public places.[95] While the courts

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

87. *Id.*

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

89. Frank X. Mullen Jr., *UNR's Camera Network Raises Fear*, RENO GAZETTE-J., Mar. 13, 2005, at 1A.

91. Jim Dwyer, *Police Video Caught a Couple's Intimate Moment on a Manhattan Rooftop*, N.Y. TIMES, Dec. 22, 2005, at B10.

92. *Id.*

94. Koskela, *supra* note 80, at 263; *see, e.g.*, Brian Roberts, *CCTV Staff 'Voyeurs'*, THE MIRROR, Dec. 7, 2005, at 9 (discussing an incident in the United Kingdom in which two municipal workers were sentenced for using surveillance cameras to film a woman undressing and being intimate with her boyfriend).

95. *See* Slobogin, *supra* note 49, at 236 n.106 (listing cases holding that

have voiced concern about the possibility of "twenty-four hour surveillance of any citizen of this country,"[96] "dragnet-type law enforcement practices,"[97] and extremely detailed aerial surveillance of intimate actions,[98] they have placed no limits on government use of video surveillance in public places.[99] Hampered as they are by standing requirements and precedent, the courts have nonetheless questioned the "compatibility of such [surveillance of public places] with desirable standards under our political form of government."[100] They have noted the manner in which video surveillance in public places raises questions about the precarious balance of state power in a democracy.[101]

Arguments against government surveillance of activities in public on freedom of speech and associational grounds have fared no better. It is well-settled that absent a compelling interest government cannot compel individuals engaged in expressive activities to divulge their identities,[102] nor can it com-

video surveillance of public areas is not a search because there is no reasonable expectation of privacy).

96. United States v. Knotts, 460 U.S. 276, 283 (1982).

97. *Id*. at 284; *see also* United States v. Garcia, 474 F.3d 994, 998 (7th Cir. 2007) ("Should government someday decide to institute programs of mass surveillance of vehicular movements, it will be time enough to decide whether the Fourth Amendment should be interpreted to treat such surveillance as a search.").

98. Dow Chem. Co. v. United States, 476 U.S. 227, 238–39 (1986) (finding that detailed aerial photographs did not raise constitutional questions, but implying that at a certain level of magnification, photographic zooming targeted at individuals as opposed to corporate activities could be so invasive as to require a warrant).

99. Katz v. United States, 389 U.S. 347, 351 (1967) ("What a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection."); Kowalski v. Scott, 126 F. App'x 558, 560 (3d Cir. 2005) ("[V]ideo surveillance . . . taken only . . . in full view of many strangers, in public areas at or near a beach[,] . . . from a distance, and in a manner that did not obstruct . . . activities[,] . . . put[s] the video surveillance in this case outside the purview of the Fourth Amendment."); United States v. McIver, 186 F.3d 1119, 1124–26 (9th Cir. 1999) (use of unmanned, motion-activated surveillance cameras on national forest land to monitor marijuana patch and identify defendant did not violate Fourth Amendment); United States v. Taketa, 923 F.2d 665, 677 (9th Cir. 1991) ("Video surveillance does not in itself violate a reasonable expectation of privacy. Videotaping of suspects in public places, such as banks, does not violate the fourth amendment; the police may record what they normally may view with the naked eye.").

100. Phila. Yearly Meeting of Religious Soc'y of Friends v. Tate, 519 F.2d 1335, 1338 (3d Cir. 1975).

101. *See, e.g.*, Bartnicki v. Vopper, 532 U.S. 514, 543 (2001) (Rehnquist, J., dissenting) (noting that private communication is essential to a democratic society).

102. *See, e.g.*, Buckley v. Am. Constitutional Law Found., 525 U.S. 182, 200

pel the disclosure of organizations' membership because of the chilling effect each would have on freedom of association and expression.[103] However, while PPVSS may be used to record images of individuals engaged in expressive activities, creating records that can be reviewed and processed (by humans or machines) to attach identities, the visual surveillance that allows this has not been found to chill expression or association.[104] In *Laird v. Tatum*, the Supreme Court held that a blatant violation of constitutional rights is not required for judicial remedy, as a mere chilling effect can be sufficient.[105] In order to be actionable, however, the Court held that the plaintiff must show concrete evidence of an actual injury.[106] While *Laird* does not necessarily preclude a finding that video surveillance could be a violation of First Amendment rights, it sets a high threshold for such a challenge.[107]

Privacy and related speech and associational concerns have been relatively unsuccessful as organizing principles in the po-

(1999) (striking down law requiring petition solicitors to wear identifying badges); Talley v. California, 362 U.S. 60, 64–65 (1960) (invalidating a ban on anonymously posted handbills).

103. *See, e.g.*, Watchtower Bible & Tract Soc'y of N.Y., Inc. v. Vill. of Stratton, 536 U.S. 150, 166–68 (2002) (holding that an ordinance requiring registration of door-to-door petitioners with local authorities violated First Amendment free expression principles); Lamont v. Postmaster Gen., 381 U.S. 301, 303–04 (1965) (holding unconstitutional a federal requirement that Post Offices maintain a list of all "communist political propaganda" recipients, and that recipients specifically state their desire to receive such "propaganda"); NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 462–63 (1958) (holding that a court order that required disclosure of organization membership rolls unconstitutional under First Amendment free association principles).

104. *But see* Slobogin, *supra* note 49, at 253 n.167 ("If cameras are equipped with parabolic audio capacity, so that they can pick up 'private' conversations on the street, their use would probably require a warrant under both the Fourth Amendment and [18 U.S.C. § 2510(2)].") (citations omitted); 18 U.S.C. § 2510(2) (2006) ("[O]ral communication [is] uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation.").

105. Laird v. Tatum, 408 U.S. 1, 12–13 (1972) ("[G]overnmental action may be subject to constitutional challenge even though it has only an indirect effect on the exercise of First Amendment rights.").

106. *Id.* at 13 ("[A party] must show that he has sustained or is immediately in danger of sustaining a direct injury as the result of [government] action." (quoting *Ex parte* Lévitt, 302 U.S. 633, 634 (1937) (per curiam))).

107. *See* Meese v. Keene, 481 U.S. 465, 472–85 (1987) (holding that the creator of work labeled "propaganda" by the government had standing to complain of a First Amendment chilling effect, but finding that no such violation occurred); ACLU v. NSA, 493 F.3d 644, 660–66 (6th Cir. 2007) (rejecting a challenge to electronic surveillance on standing grounds).

litical process as well. Several scholars have noted the difficulty privacy issues face in the political sphere.[108] While some jurisdictions have abandoned video surveillance systems because they have proven unhelpful, we know of no jurisdiction that has rejected a video surveillance system or dismantled one due to privacy concerns. In fact, police and local governing bodies frequently describe communities demanding cameras be installed.[109] Given that communities entrust law enforcement with firearms, arguments to deny them the use of video cameras, even those permanently installed, face an uphill battle.

Privacy and "chilling effect" objections to video surveillance of public places are descriptively unsatisfying. They are both vague and ambiguous. They problematize the use of vision-enhancing technology by the police in public places generally—if video surveillance systems violate privacy, do stand-alone cameras violate it as well? What is the "reasonable expectation of privacy" that the Fourth Amendment ought to protect in publicly observable acts occurring in public places? And how should it constrain police use of sight-enhancing technology? Vague notions of privacy give us little guidance about how often or intensely an officer may watch without raising concerns. Prohibiting the police from using technology to enhance safety due to concerns about privacy and First Amendment freedoms seems both unlikely as a political matter, and difficult to justify considering the relative value put on privacy and freedom of expression compared to physical security and the states' obligation to secure each according to international human rights norms.[110] Privacy and freedom of expression are derogable rights—the state may interfere with them to protect other rights and freedoms.[111] We need a better framework for govern-

108. *See* PRISCILLA M. REGAN, LEGISLATING PRIVACY 210–11 (1995) (arguing that privacy fails to gain support in federal legislative battles unless tied to promoting another value such as access to health care); Goold, *supra* note 61 (discussing failure of privacy described as individual right to gain traction with the public and arguing for privacy's value in a free society).

109. *See supra* note 45 (discussing efforts to gain community participation in the decision to use surveillance equipment).

110. *See, e.g.*, International Convention on Civil and Political Rights art. 4.2, Dec. 16, 1966, S. TREATY DOC. NO. 95-20, 999 U.N.T.S. 171 (excluding privacy and free expression rights from rights that are not to be derogated in a public emergency, but including rights of physical integrity).

111. *Cf.* U.N. Econ. & Soc. Council [ECOSOC], Comm'n on Human Rights, *Johannesburg Principles on Nat'l Sec., Freedom of Expression & Access to Info.*, ¶1.2, U.N. Doc. E/CN.4/1996/39 (Mar. 22, 1996) (discussing conditions and limitations under which states may interfere with derogable rights to protect

ing state use of surveillance technology.

III. EVALUATING PERMANENT PUBLIC VIDEO SURVEILLANCE SYSTEMS FROM THE PERSPECTIVE OF POLICING IN A DEMOCRACY

A then-newly appointed Justice Rehnquist wrote, "[i]n Hitler's Germany and Stalin's Russia, there was very efficient law enforcement, there was very little privacy, and the winds of freedom did not blow."[112] Although privacy often gave way to law enforcement needs during his tenure on the Court,[113] in his 1974 article discussing a low-tech surveillance scheme in which police routinely and without justification recorded the license plates of bar patrons he wrote that the "interest in not having public activities observed and recorded may prevail in the absence of any governmental justification for the surveillance."[114] His conclusion was not based on a privacy claim, but rather on a broader belief that such information-gathering was "simply not the kind of governmental interest that ought to rate high in a free society."[115] The conservative *New York Times* columnist and former Nixon speechwriter William Safire echoed this sentiment when he wrote: "[t]o be watched at all times, especially when doing nothing seriously wrong, is to be afflicted with a creepy feeling. . . . It is the pervasive, inescapable feeling of being unfree."[116]

A rich literature connects surveillance with oppressive state control. Yet, today, states considered strong democracies sport vast surveillance infrastructures. For example, since the attacks of September 11, 2001, the United States has invested billions in technology to extract information and monitor the

national security); U.N. Econ. & Soc. Council [ECOSOC], Sub-Comm'n on Prevention of Discrimination & Prot. of Minorities, *Siracusa Principles on the Limitation & Derogation of Provisions in the Int'l Covenant on Civil & Political Rights*, ¶39, U.N. Doc. E/CN.4/1985/4 (Sept. 28, 1984) (discussing conditions and limitations under which states may interfere with derogable rights in the case of a public emergency).

112. William H. Rehnquist, *Is an Expanded Right of Privacy Consistent with Fair and Effective Law Enforcement? Or: Privacy, You've Come a Long Way, Baby*, 23 U. KAN. L. REV. 1, 21 (1974).

113. *See* Susan M. Gilles, *From Rehnquist to Roberts: Has Information Privacy Lost a Friend and Gained a Foe?*, 91 MARQ. L. REV. 453, 474–77 (2007) (discussing Rehnquist's perspective on privacy in relation to law enforcement).

114. Rehnquist, *supra* note 112, at 14.

115. *Id.* at 11.

116. William Safire, *The Great Unwatched*, N.Y. TIMES, Feb. 18, 2002, at A15.

population, and it is not alone.[117] The United Kingdom has so many cameras monitoring its public places that a citizen is supposedly caught on camera over three hundred times a day.[118] The United Kingdom has recently moved to integrate automatic vehicle identification technology into the camera networks.[119] The use of advanced technologies by democratic states to engage in generalized surveillance of the population forces us to consider what is necessary to maintain states' democratic nature. As an increasing number of scholars rightly note, the question is not whether we will have a surveillance society, but rather what kind it will be.[120]

To answer this question we need to understand how various technologies alter the balance of power between citizens and police; in particular how the use of a specific remote sensing technology loosens traditional constraints on the state's exercise of power. For our purposes, we examine how permanent public video surveillance systems alter the citizens' experience in relation to the policing of public places.

117. *See, e.g.*, Jason Ryan, *DOJ Budget Details High-Tech Crime Fighting Tools: New Surveillance Programs Look Ahead as FBI Seeks to Overcome Past Criticism*, ABC NEWS, May 9, 2009, *available at* http://abcnews.go.com/TheLaw/story?id=7532199 (discussing costs during 2010 for FBI, DOJ, and DoD projects including $233.9 million for "Advanced Electronic Surveillance" and $97.6 million for a "Biometric Technology Center" with full deployment costing "up to $1 billion"); *see also* Electronic Privacy Information Center, U.S. Domestic Surveillance Budget Fiscal Year 2006, http://epic.org/privacy/budget/fy2006/ (last visited Feb. 13, 2010) (reporting, among other allocations, $41.1 billion to the Department of Homeland Security, $847 million for an office of Screening Coordination and Operations, which would oversee vast databases of digital fingerprints and photographs, eye scans, and personal information from millions of Americans and foreigners; $20 million for the Border Patrol for sensors, communication, and video surveillance capabilities; $51.1 million for America's Shield Initiative, which enhances electronic surveillance capabilities along U.S. borders; and $3 million for a system that captures biometric and biographical information).

118. A REPORT ON THE SURVEILLANCE SOCIETY: FOR THE UNITED KINGDOM INFORMATION COMMISSIONER BY THE SURVEILLANCE STUDIES NETWORK 19 (David Murakami Wood ed., 2006) ("[T]here may now be as many as 4.2 million CCTV cameras in Britain: one for every fourteen people, and a person can be captured on over three hundred cameras each day.").

119. Norris Statement, *supra* note 51, at 35–36.

120. *See, e.g.*, Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 17 (2008) (arguing that the choice to be made is not whether to have a national surveillance state or not, but between a democratic or authoritarian version of that state).

A. PERMANENT PUBLIC VIDEO SURVEILLANCE ALTERS PUBLIC PLACES

Bentham and Foucault vividly described the coercive power produced by the possibility of constant observation.[121] In their explorations, the coercive power of observation was brought about through the intentional architectural design of specific correctional institutions.[122] Shielding the identity and activities of the watchers, while simultaneously placing subjects in a position of constant exposure yielded an environment where surveillance *felt* constant.[123] Through the constant possibility of surveillance the physical space would lead the watched to internalize the social norms of their watchers.[124] The desired outcome was reformed citizens who could be expected to safely re-enter society, imbued with a newfound fidelity to social norms.[125]

Today our public places are receiving a significant, although less visible, architectural redesign that, like Bentham's Panopticon, presents the possibility of constant surveillance. Aimed not at individuals housed in institutions and deemed in need of reformation, but at the broad public as it commutes, shops, meanders, and plays, surveillance cameras are altering the architecture of our public places. One can no longer assume that the absence of other individuals from a public place affords solitude or privacy. One may be physically alone, yet fully observed. In place of the human observer, a stalwart electronic eye connected to an infallible, perhaps boundless, memory watches over the public square.

The introduction of permanent public video surveillance

121. JEREMY BENTHAM, PANOPTICON: OR, THE INSPECTION-HOUSE, at iii (Dublin, Thomas Byrne 1791) ("[The Panopticon is a] new mode of obtaining power, of mind over mind, in a quantity hitherto without examination."); Michel Foucault, *The Eye of Power*, *in* POWER/KNOWLEDGE 146, 155 (Colin Gordon ed., Pantheon Books 1980) (1972) ("An inspecting gaze, a gaze which each individual under its own weight will end by interiorizing to the point that he is his own overseer.").

122. *See* JEREMY BENTHAM, POSTSCRIPT PART I CONTAINING FURTHER PARTICULARS AND ALTERATIONS RELATIVE TO THE PLAN OF CONSTRUCTION ORIGINALLY PROPOSED; PRINCIPALLY ADAPTED TO THE PURPOSE OF A PANOPTICON PENITENTIARY-HOUSE, *reprinted in* BENTHAM, *supra* note 121 (describing the construction of the proposed Panopticon prison).

123. Foucault, *supra* note 121, at 147–48.

124. *See* Haggerty & Ericson, *supra* note 74, at 607 (arguing that the "disciplinary aspect of panoptic observation" encourages "productive soul training").

125. BENTHAM, *supra* note 121, at 66.

systems[126] changes the terms of participation in public places—what an individual is presumed to have agreed to when "knowingly expos[ing]"[127] herself to the public. There are six distinct, yet interrelated aspects to the shift in the relative balance of power between the state and the citizen.

1. The State's Gaze Becomes Unrelenting

Previously an individual's presence in a public place made her temporarily visually and physically accessible to law enforcement, raised the possibility that she would be noticed or identified, and in a rare instance "sniffed,"[128] recorded,[129]

126. THE CONSTITUTION PROJECT, *supra* note 65, at 46 ("Permanent Public Video Surveillance System[s are] . . government owned and operated video cameras focused on a public place, . . . implemented for an indefinite period of time . . . and the primary purpose of which extend beyond a single, specific law enforcement investigation."). Video footage is increasingly captured, stored and shared by individuals and organizations in the private sector due to the increasing ubiquity of video capture on devices such as mobile phones and cameras, the explosion in services for sharing videos, and the increasing use of surveillance systems for organizational security. *See supra* notes 86–88 and accompanying text. There are important questions about the access and use of the government to privately captured video images. In addition, there is a rise in hybrid systems—those installed by private parties at the direction of the government and with direct or indirect government access facilitated. *See infra* note 227. However, the PPVSS is the paradigmatic case. We save the issues raised by other forms of increased surveillance of public places for a later date.

127. Katz v. United States, 389 U.S. 347, 351 (1967) ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.").

128. *See, e.g.*, Illinois v. Caballes, 543 U.S. 405, 408 (2005) (noting that there are some instances where police use of a drug-sniffing dog would qualify as a search within the meaning of the Fourth Amendment, but holding that "a traffic stop that is lawful at its inception and otherwise executed in a reasonable manner" is not unconstitutional); United States v. Place, 462 U.S. 696, 700–08 (1983) (holding that in the context of luggage temporarily seized at an airport, a canine sniff is not a search within the meaning of the Fourth Amendment so long as the traffic stop is "lawful at its inception and otherwise executed in a reasonable manner").

129. *Cf. Katz*, 389 U.S. at 353 (holding that the interception of a conversation in which a person has a reasonable expectation of privacy constitutes a search within the meaning of the Fourth Amendment even if it occurs in a public place). When considering whether a person has a reasonable expectation of privacy in the context of eavesdropping, courts have applied a number of factors. First is "the volume of the communication or conversation." Kee v. City of Rowland, 247 F.3d 206, 213 (5th Cir. 2001); *see also* United States v. Burns, 624 F.2d 95, 100 (10th Cir. 1980) (holding that there is no reasonable expectation of privacy in a hotel room conversation loud enough that it could be heard in adjoining rooms); United States v. Agapito, 620 F.2d 324, 329 (2d Cir. 1980) (similar holding); Kemp v. Block, 607 F. Supp. 1262, 1264 (D. Nev.

stopped and searched,[130] asked to divulge her name,[131] or, on rare occasions, arrested.[132] Today, the consequences of being in public are far greater, and the information provided to individ-

1985) (holding that arguing loud enough to be overheard by coworkers undermines a reasonable expectation of privacy). Second is "the proximity or potential of other individuals to overhear the conversation." *Kee*, 247 F.3d at 213–14; *see also In re* John Doe Trader No. One, 894 F.2d 240, 243 (7th Cir. 1990) (finding no reasonable expectation of privacy for comments made on commodities exchange floor). Third is "the potential for communications to be reported." *Kee*, 247 F.3d at 214; *see also* United States v. White, 401 U.S. 745, 749 (1971) (finding an inherent risk that any conversation will be reported to authorities); Hoffa v. United States, 385 U.S. 293, 303 (1966) ("The risk of being overheard by an eavesdropper or betrayed by an informer . . . is probably inherent in the conditions of human society." (quoting Lopez v. United States, 373 U.S. 427, 465 (1963))); United States v. Longoria, 177 F.3d 1179, 1183 (10th Cir. 1999) ("[Defendant] had no reasonable expectation that the person in whose presence he conducts conversations will not reveal those conversations to others. He assumed the risk . . . ."). Fourth are "the affirmative actions taken by the speakers to shield their privacy." *Kee*, 247 F.3d at 214; *see also Katz*, 389 U.S. at 363 n.* (White, J., concurring) ("[A]s the Court emphasizes the petitioner 'sought to exclude . . . the uninvited ear.'"); United States v. Smith, 978 F.2d 171, 177 (5th Cir. 1992) ("While it is true that the right to privacy in a personal conversation is generally a reasonable expectation, the actions of the parties to the conversation may reduce this expectation to the point that it is no longer 'reasonable'"). Fifth is "the need for technological enhancements to hear the communications." *Kee*, 247 F.3d at 214; *see also Agapito*, 620 F.2d at 330 n.7 ("The absence of electronic eavesdropping of course is significant. . . . 'There is a qualitative difference between electronic surveillance . . . and conventional police strategems such as eavesdropping.'" (quoting *Lopez*, 373 U.S. at 465 (Brennan, J., dissenting))). Sixth is "the place or location of the oral communications as it relates to the subjective expectations of the individuals who are communicating." *Kee*, 247 F.2d at 214–15; *see also* Minnesota v. Carter, 525 U.S. 83, 88 (1998) ("[T]he extent to which the Fourth Amendment protects people may depend upon where those people are.").

130. In *Terry v. Ohio*, 392 U.S. 1 (1968), and its progeny, the Supreme Court has established what amounts to a constellation of data points, rather than a firm and easily deployed test, for determining whether a warrantless investigative stop—now generally called a *Terry* stop—is valid under the Fourth Amendment's reasonableness requirement. The Court has made clear that the constitutionality of a warrantless stop-and-frisk depends largely on the particular facts of the case. *See, e.g.*, United States v. Cortez, 449 U.S. 411, 417–18 (1981) ("[T]he detaining officers must have a particularized and objective basis for suspecting the particular person stopped of criminal activity."); *see also* Terry v. Ohio *30 Years Later*, 72 ST. JOHN'S L. REV. 721 (1998) (providing a comprehensive analysis of *Terry* by a wide variety of commentators).

131. Hiibel v. Sixth Judicial Dist. Court, 542 U.S. 177, 188–89 (2004) ("[T]he request for identification was 'reasonably related in scope to the circumstances which justified' the stop. . . . The stop, the request, and the State's requirement of a response did not contravene the guarantees of the Fourth Amendment." (quoting *Terry*, 392 U.S. at 20)).

132. United States v. Watson, 423 U.S. 411, 414–24 (1976) (holding that an individual can be arrested in a public place without a warrant based on probable cause that they have committed or are about to commit a crime).

uals about those consequences are far less.

Unlike police officers, PPVSS notice everything that occurs in its field of view.[133] An individual and his activities will be noticed regardless of how mundane or dramatic his appearance and behavior. The documentation of presence and action becomes routine—requiring no ex ante judgment by the state as to the utility of the information. Bounded, if at all, by ever-decreasing economic limitations[134] the paradigm shifts from "relative inattention to relative attention"[135] as cameras indiscriminately capture all in its field of view.

2. Temporal Constraints on Policing Are Lifted

The introduction of the PPVSS alters the temporality of public exposure. It does so in two distinct ways. First, the ephemeral and transient nature of presence and action in the public place dissolves as recorded images memorialize both.[136] Second, the captured images remove temporal restrictions on policing activities.[137] The availability of video footage supports asynchronous vision, granting police hindsight. In this way, video surveillance systems can flatten time. An individual's presence in a space is retrievable in any point in the future. Video surveillance footage brings the present into the future. The captured images turn the individual's transient presence in a public place into a permanent state of exposure. The de-

133. *See, e.g.*, Kevin Werbach, *Sensors and Sensibilities*, 28 CARDOZO L. REV. 2321, 2365 (2007).

134. *Cf.* Liza Vertinsky & Todd M. Rice, *Thinking About Thinking Machines: Implications of Machine Inventors for Patent Law*, 8 B.U. J. SCI. & TECH. L. 574, 578 (2002) (discussing Moore's Law, the term for the phenomenon of computer processing speeds that double every eighteen months for the same cost).

135. *See* Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 423 (1980) ("Our interest in privacy, . . . is related to our concern over our accessibility to others: the extent to which we are known to others, the extent to which others have physical access to us, and the extent to which we are the subject of others' attention."); *id.* at 428 ("A loss of privacy occurs as others obtain information about an individual, pay attention to him, or gain access to him. These three elements of secrecy, anonymity, and solitude are distinct and independent, but interrelated . . . ."); *id.* at 432 ("[A]ttention alone will cause a loss of privacy even if no new information becomes known.").

136. Werbach, *supra* note 133 ("[V]enturing out in public is now an activity that creates a real possibility of being tracked, or of having images captured that could be used in some other context later. . . . [T]he idea that anything visible will go unnoticed is becoming less realistic.").

137. *See id.* at 2343 (discussing examples of authorities using privately captured images to identify perpetrators after the fact).

fault state of transient, nonrecorded passage or presence is replaced by routine documentation of the individual's presence in public places.[138] A fine can be levied, or an arrest made, despite the absence of a witness to the offending act in real-time.[139] In addition to temporal constraints being lifted, spatial constraints also become inapplicable.

3. Spatial Constraints on Policing Are Lifted

The physical boundaries of public places under surveillance are unknown to those occupying the place. Surveillance cameras remove physical barriers to visual accessibility allowing remote viewing.[140] Like telephoto lenses and binoculars, but more so, PPVSS unify physically discrete spaces.[141] The contours of the physical place dissolve as the network of cameras invisibly structures and restructures lines of sight—mapping new places in two dimensions creates continuity between spaces that are physically removed from one another. This allows

138. *See* Patricia L. Bellia, *The Memory Gap in Surveillance Law*, 75 U. CHI. L. REV. 137, 140 (2008) (discussing the implications of the shift from "an architecture of forgetting" to "an architecture of memory" in the commercial sector in light of the current surveillance law framework distinction between direct and indirect government surveillance).

139. *See* JOHN S. ADAMS & BARBARA J. VANDRASEK, CTR. FOR TRANSP. STUDIES, AUTOMATED ENFORCEMENT OF RED-LIGHT RUNNING & SPEEDING LAWS IN MINNESOTA: BRIDGING TECHNOLOGY AND PUBLIC POLICY 12 (2009), http://www.cts.umn.edu/Publications/ResearchReports/pdfdownload.pl?id=1234 (discussing legal approaches to automated red-light camera ticketing systems); Norris Statement, *supra* note 51, at 36 (discussing use of automatic number plate recognition and surveillance cameras to make 10,000 arrests in a United Kingdom test).

140. Professor Gavison claims that privacy can be conceptualized as concerns about three forms of accessibility: "the extent to which we are known to others" (information privacy); "the extent to which others have physical access to us" (contact or observation with normal senses); and "the extent to which we are the subject of others' attention" (monitoring, regardless of proximity or information collection). Gavison, *supra* note 135, at 423. Her conceptualization of privacy is helpful in exploring the various ways in which surveillance camera systems interact with privacy, however her views on physical access seem limited given the ability to exercise control over an individual or their environment remotely. Gavison distinguishes this point by saying that even if the information acquired on, and attention afforded to, the individual remains unchanged, the physical accessibility alters privacy by diminishing "spatial aloneness." *Id*. at 433. However, why should the "ability to watch and listen," *id*., from a distance not alter the physical access dimension of privacy?

141. *See generally* Cohen, *Cyberspace*, *supra* note 61 (discussing "networked space" and its social implications); Timothy Zick, *Clouds, Cameras, and Computers: The First Amendment and Networked Public Places*, 59 FLA. L. REV. 1 (2007) (exploring negative First Amendment implications of networked public places).

the police to have sight without presence. The officer may be able to bear witness to harm, yet is too far removed to intervene. At the same time, the presence of the cameras may convince individuals in the public place to act less cautiously because they believe the cameras are monitored and assistance will appear if criminal activity erupts. Depending upon whether and how individuals are aware of the responses triggered by the cameras they may come to conclude that the unblinking eye presents either the all-seeing eye of the state or the blind eye of the Cyclops. This eye has enhanced PPVSS capabilities.

4. PPVSS Increase the Acuity and Breadth of the State's Gaze

Modern surveillance cameras, with the ability to pan, tilt, and zoom, allow police to place individuals under a microscope and simultaneously enjoy a birds-eye view. As discussed above, and noted by advocates,[142] the disintermediation of sight allows police visual access to actions and information that individuals would choose to shield or cease to engage in if the police presence was known. For example, faced with a physically present police officer, it seems likely that individuals would shield the screen of their computer or close their book. The zoom feature of PPVSS allows police to violate normative constraints on their activities in physical space. The acuity of the state's gaze is magnified because the state is invisible. At the same time, the state's gaze gains breadth. Everyone may be subject to constant surveillance and constant recording whether walking across Main Street, walking through an alleyway, or ducking into the lobby of a bank. The birds-eye view removes many of the ground-level architectural elements that limit visual access and identification of those being surveilled.

5. PPVSS Increase the Possibility of Identification

Recording the images of individuals and events in public places expands opportunities for identification. People who express themselves in public—politically or otherwise—know they will be observed. While many do not wear masks or otherwise actively disguise themselves, they enjoy "relative inattention" from police and other strangers.[143] Video surveillance can nullify that anonymity. Because a state-of-the-art digital camera images are far better than a government agent's memory or

142. *See supra* notes 140–141 and accompanying text.

143. *Cf.* Slobogin, *supra* note 49, at 239.

handwritten notes, the government's ability to link faces with names vastly improves.[144] Furthermore, constant surveillance of a person's movements—now possible with panoramic video surveillance of large swaths of city centers[145]—can reveal associations, addresses, and locales that divulge that person's identity.

An excellent example of this shift in power comes from the University of Colorado-Boulder, where students at a marijuana "smoke-in" found themselves in a high-tech lineup when police derived mug shots of participants from video surveillance tape of the event and offered rewards to the public for their identification.[146] The students had felt a sense of safety and relative anonymity in the crowd, despite signs that proclaimed the video surveillance of the space.[147] The mixture of video surveillance and human processing—peer production—allowed the police to quickly identify and fine individuals at little cost to the department.[148] The loss of anonymity was due not to the recording of the images independently, but because digital recording allowed them to be processed and in an asynchronous manner. Police have traditionally used a host of investigative techniques that rely on external sources of knowledge to identify both perpetrators and victims, from "Wanted" posters ubiquitous in post offices around the country to shows like *America's Most Wanted*.[149] Each method attempts to leverage community knowledge on a large scale; however, the Boulder example, because it leveraged the Internet, produced participation and results at an unprecedented scale and speed.

Similarly, even in the absence of identification, in a formal sense, PPVSS increase the state's ability to profile individuals.[150] Video surveillance footage can facilitate the aggregation

144. *See* Lillie Coney, Elec. Privacy Info. Ctr., Expectations of Privacy in Public Spaces, Statement to Dep't of Homeland Sec. Data Privacy & Integrity Advisory Comm. 2–8 (2006), *available at* http://epic.org/privacy/surveillance/coneytest060706.pdf (comparing strengths and limitations of police officers and video surveillance and the ramifications for privacy and expressive activity).

145. *See* Burrows, *supra* note 66, at 1079–81.

146. RYAN SHAW, RECOGNITION MARKETS AND VISUAL PRIVACY 1 (2006), *available at* https://www.law.berkeley.edu/bclt/events/unblinking/unblinking/shaw.pdf.

147. *Id.* at 1.

148. *Id.*

149. *See id.*

150. *See* Heidi Mork Lomell, *Targeting the Unwanted: Video Surveillance and Categorical Exclusion in Oslo, Norway*, 2 SURVEILLANCE & SOC'Y 346,

of an individual's presence and actions at distinct times and places into a composite or selectively edited dossier.[151] Today such documentation does not produce absolute visibility because neither man nor machine is capable of turning the massive number of images captured into reliable narratives at the scale and timeframe required; however, this will change as image processing and identification techniques improve.[152]

6. PPVSS Destroy the Mutuality of Visual Accessibility

Like the Panopticon, the inability to know whether or when one is observed is a critical design feature of the video surveillance environment.[153] While some video surveillance cameras may be accompanied by a sign declaring the area under surveillance, the blank eye of the camera, positioned high over head, provides little information about what is being viewed, or at what level of detail.[154] The watcher can be at great physical remove from the watched, eliminating the reciprocity of potential visibility experienced in nonnetworked space.[155] The police may have visual access to a public place but the individuals occupying the space cannot tell.[156] Police may be actively viewing the cameras, panning, tilting, and zooming to follow various individuals in the public place, yet everyone in the public place is left unaware.[157] PPVSS changes the nature of people's interactions with the government.

B. IMPLICATIONS OF PPVSS FOR THE RELATIONSHIP BETWEEN STATE AND CITIZEN

Each of these changes to the public place alters the relationship between the state and the citizen—each enhances the power of the state.[158] Scholars have suggested various responses

351–53 (2004), *available at* http://www.surveillance-and-society.org/articles2(2)/unwanted.pdf.

151. *See* SHAW, *supra* note 146, at 3.

152. *See id*. at 5.

153. *See* Hille Koskela, *'Cam Era'—The Contemporary Urban Panopticon*, 1 SURVEILLANCE & SOC'Y 292, 294 (2003), *available at* http://www.surveillance-and-society.org/articles1(3)/camera.pdf.

154. *See id*. at 298–99.

155. *See id*.

156. *See id*.

157. *See id*.

158. *See, e.g.*, SELECT COMMITTEE ON THE CONSTITUTION, SURVEILLANCE: CITIZENS AND THE STATE, 2008-9, H.L. 18–I, at 6 (emphasizing how surveillance and data collection can alter "the nature of citizenship in the 21st century, especially in terms of citizens' relationship with the state").

to this shift. For example, some, such as David Brin, have argued that the alternative to the rise of state video surveillance is "sousveillance"—observing from below.[159] The antidote is to make sure that citizens can observe the state.[160] Steve Mann has devoted his life work toward this end—relentlessly documenting events from his perspective—visually, aurally, and with an increasing range of sensory enhancements.[161] Christopher Slobogin has proposed taking the Court's position that society's views are relevant by defining the Fourth Amendment in terms of "expectations of privacy society is prepared to recognize as reasonable" and through empirical research providing support for the claim that individuals consider PPVSS to be as intrusive as other police tactics regulated by the Fourth Amendment, concluding PPVSS should be regulated too.[162] Anthony Amsterdam proposes that courts balance unregulated police surveillance with the resulting decline in the amount of privacy and freedom of the public to determine surveillance's consistency with the "aims of a free and open society"[163] Marc Blitz further proposes an "architecture-based approach" to interpreting the Fourth Amendment that would direct the court to consider whether a given technology erodes "the privacy- and anonymity-enabling features of public space" below what is necessary to "to guarantee that the public sphere retains a character that continues to provide individuals the opportunities to preserve privacy where they believe they need it."[164] Gary Marx reviews techniques of *neutralization*—defined as "direct resistance or avoidance rather than a broad strategic response"

159. *See* DAVID BRIN, THE TRANSPARENT SOCIETY: WILL TECHNOLOGY FORCE US TO CHOOSE BETWEEN PRIVACY AND FREEDOM? 3–8 (1998).

160. *See id.*; *see also* DANIEL J. WEITZNER ET AL., MASS. INST. OF TECH. COMPUTER SCI. & ARTIFICIAL INTELLIGENCE LAB. TECHNICAL REPORT, TRANSPARENT ACCOUNTABLE DATA MINING: NEW STRATEGIES FOR PRIVACY PROTECTION 1–3 (2006), *available at* http://hdl.handle.net/1721.1/30972 (proposing a regime of transparent and accountable usage rules to replace the dominant privacy focus on limiting access).

161. *See* Steve Mann, *"Sousveillance": Inverse Surveillance in Multimedia Imaging*, *in* PROCEEDINGS OF THE 12TH ANNUAL ACM INTERNATIONAL CONFERENCE ON MULTIMEDIA 620, 621–22 (2004).

162. Slobogin, *supra* note 49, at 271–86 (discussing the results from a survey of 190 individual jurors in which the jurors rated the intrusiveness of various activities). Slobogin also advances First Amendment and Due Process Clause theories for limiting pervasive video surveillance. *See id.* at 252–67.

163. Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 403 (1974).

164. Blitz, *supra* note 76, at 1422–23.

commonly used to counter surveillance.[165] Colin Bennett's recent book, *The Privacy Advocates*, provides insight into the variety of frames and techniques used to countersurveillance in the political realm.[166]

This Article advances a different line of inquiry, asking what democratic theory as expressed in criminal procedure and other institutional constraints on policing suggests should concern us about the changes outlined in Part III.A. Framed as constraints—rather than resistance, neutralization, or counterstrategies—these next sections identify the checks and balances that may allow society to reap the benefits of PPVSS (and other technologies that law enforcement employs) while staving off the dystopian worlds so fully presented in literature and film.[167] Building upon insights into the connections between various strains of democratic theory, developments in criminal procedure, and approaches to managing institutions of policing identified by David Sklansky in his article,[168] Part III considers how PPVSS challenge mechanisms used to manage the tension between policing and democracy. Through this analysis we attempt to provide a partial answer to the question of how to distinguish a democratic from a totalitarian surveillance state.[169]

1. Democratic Theory and Policing

In *Police and Democracy*, David Sklansky unearths and details the connections between theories of democracy and criminal procedure and other institutional constraints on police power and practice.[170] He connects developments in criminal

165. Gary T. Marx, *A Tack in the Shoe and Taking off the Shoe: Neutralization and Counter-neutralization Dynamics*, 6 SURVEILLANCE & SOC'Y 295, 297 (2009), *available at* http://www.surveillance-and-society.org/ojs/index.php/journal/article/view/shoe/shoe.

166. COLIN J. BENNETT, THE PRIVACY ADVOCATES: RESISTING THE SPREAD OF SURVEILLANCE 1–25 (2008).

167. For example, BRAZIL (Universal Studios 1985); ENEMY OF THE STATE (Touchstone Pictures 1998); GATTACA (Columbia Pictures 1997); GEORGE ORWELL, 1984 (Signet Classics 1981) (1949); MINORITY REPORT (20th Century Fox 2002).

168. *See* David Alan Sklansky, *Police and Democracy*, 103 MICH L. REV. 1699, 1702–08 (2005).

169. Our analysis yields only a partial response because questions about the rule of law, the relative strength of the underlying structures that support a strong democracy—for example, an independent judiciary—and questions about the substantive laws and policies the surveillance is used to implement are beyond the scope of this Article.

170. *See* Sklansky, *supra* note 168, 1703–05.

procedure such as reliance on judicial oversight to limit police discretion, an emphasis on community participation in policing decisions and desire for transparency of policing strategies, and efforts to eliminate bias and systems of domination to strains of democratic theory dominant at various times in the United States.[171]

His work to draw connections between understandings of democracy and the constraints they have historically produced on police and policing provide a helpful tool for considering what aspects of PPVSS ought to concern societies committed to democracy.[172] This is beneficial in three ways. First, it focuses the analysis on power rather than privacy.[173] Moving the discussion about government use of permanent public video surveillance systems away from privacy, anonymity, and related expressive and associational rights, towards a conversation about how these systems challenge central tenets of criminal procedure and citizen-police relations—transparency, discretion, oversight, and accountability—will clarify the issues and the means of addressing them.[174] Second, this focus will yield greater political engagement because it does not polarize the issue into a debate about whether individuals maintain any expectations of privacy against observation in public places.[175] Third, it provides guidance that can be used to shape the technology police use, as discussed in Part IV, as well as policies to govern its use.[176]

Sklansky discusses three strands of democratic theory—pluralism, deliberation, and anti-egalitarianism.[177] For each theory he examines developments in criminal procedure, approaches to managing the police, and scholarly work on policing during the period in which the theory held greatest sway.[178]

171. *Id*. at 1709 (considering the "*purposes*, *processes*, *proximity*, and *particularity*" of various theories of democracy).

172. *See id*. at 1704–08.

173. *Cf*. Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 127 (2004) ("To the extent that protecting privacy against government intrusion can be portrayed as an insurance policy against the emergence of totalitarianism, the rhetoric of limiting government powers can be parlayed into protection of privacy.").

174. *See* Sklansky, *supra* note 168, at 1705–08.

175. *See id*. at 1808.

176. *See id*. at 1809–10.

177. *See id*. at 1705–06.

178. *See id*. (providing an overview of the connections between various theories of democracy and "jurisprudential and academic discussions of the police").

Through an analysis of the aims of each democratic theory he is able to more concretely assert connections to developments concerning policing.[179] For our purposes, relevant developments in the field of criminal procedure and policing more broadly, which Sklansky connects to theories of democracy, include transparency of police practices; external limits on police discretion through oversight by elites, specifically judicial oversight; community participation in policing; and the elimination of bias and systems of domination.[180]

2. Ramifications of PPVSS Relevant to Democratic Theory and Policing

Part III outlined the manner in which PPVSS alter the terms of interaction between the police and citizen in public places.[181] The alterations PPVSS bring to the police-citizen relationship challenge––and at times directly undermine––the checks on policing that are rooted in democratic theory.

a. PPVSS Reduce Transparency

PPVSS reduce the information available to the public about policing practices and policies. As discussed in Part I, at the highest level the funding of PPVSS through federal grants frequently skirts the political processes at the local level, reducing the affected communities' access to information about the

179. With respect to the theory of pluralism, he finds the aims to be social stability, group competition, the promotion of personal dignity, and the avoidance of authoritarianism; with respect to participatory and deliberative democratic theories, he finds the aims to be fomenting grassroots politics and promoting deliberation by the community; and, with respect to the anti-inegalitarianism strand of democratic theory, he finds the aims to be ongoing reforms against inequality, the important role of resistance politics, and the recognition of the importance of police as a unique tool for either perpetuating or halting hegemonic domination. *See id*. at 1706.

180. *See id*. at 1781 (connecting "enthusiasm for community participation, a premium placed on transparency" with the rise of theories of participatory democracy and deliberative democracy); *id*. at 1731 (arguing that "outlook of democratic pluralism *was* reflected in Warren and Burger Court criminal procedure," specifically through external limits on police discretion through oversight by elites and "the concern with police discretion and the reliance on judicial oversight") (emphasis added); *id*. at 1807–09 (discussing the relative inattention of dominant democratic theories to issues of equality and suggesting that a more well-rounded understanding of democracy would take "democratic-oppositionalism" into account with its focus on the elimination of bias and systems of domination).

181. *See supra* Part III.A.

systems.[182] Once in use, PPVSS reduce the need for police to be physically present to impact an area.[183] PPVSS make it difficult to assess the whereabouts of the police.[184] While the presence of cameras in a locale sends a coarse signal of a police presence, it provides no information about whether police are actively surveilling an area at a given time.[185]

The ability to closely observe individuals while remaining hidden reduces information about who is being watched.[186] This in turn limits the ability of the community's sensibilities to inform police practices. Unless there are active measures to force transparency, police practices relating to PPVSS are largely inscrutable.[188]

b. Increase in Unchecked Discretion

PPVSS also allows police to single out individuals and subject them to intense scrutiny when in public places without either seizing or searching them.[189] To date the courts have not placed limits on the acuity, intensity, or longevity of police officers' visual observation of individuals in public places.[190] Therefore, police are relieved of judicial oversight, which acts as an ex ante check on forms of investigation that are considered to be searches. In addition to being exempt from the formal procedural constraints that attend a search, police also escape the practical limits that act as a check on their use of

182. *See supra* text accompanying notes 23–24.

183. *Cf.* ADAMS & VANDRASEK, *supra* note 139, at 15–18 (discussing the impact of using speed cameras to enforce speed limits).

184. *See* Koskela, *supra* note 69, at 249.

185. *Id.*

186. *Id.*

188. The San Francisco Camera Ordinance forces transparency at various stages of the PPVSS process. *See* discussion *infra* Part IV.A. It requires a public hearing prior to the installation of cameras, it requires notice to be provided to individuals in affected areas, as well as notices on the cameras themselves, and, perhaps most importantly, it requires the police department to report on the use of the system at periodic intervals providing a mechanism for ongoing public oversight. S.F., CAL., ADMIN. CODE §§ 19.1–19.7 (2006). In a similar vein, the federal government is required to report on its use of wiretaps. *See* Paul M. Schwartz, *Reviving Telecommunications Surveillance Law*, 75 U. CHI. L. REV. 287, 289–91 (2008) (discussing reporting requirements and gaps of federal wiretap laws and advocating for additional reporting requirements).

189. *See* E. Casey Lide, *Balancing the Benefits and Privacy Concerns of Municipal Broadband Applications*, 11 N.Y.U. J. LEGIS. & PUB. POL'Y 467, 476–77 (2008).

190. *See id.* at 482.

power. Unlike a *Terry* stop,[191] which can also occur without prior judicial authorization, individuals subject to intense visual surveillance may remain completely unaware of the police attention.[192] The invisibility of the police action limits the ability of the community to notice the police encounter and reduces the community's ability to complain about police practices or enforce nonjudicial constraints.[193]

c. PPVSS Seem Particularly Likely to Enhance Bias

PPVSS naturally focus police—as they do others—on visible traits such as race, age, gender, and dress in ways that seem likely to heighten rather than mitigate bias in police decisions. Researchers have documented the use of surveillance systems to sanitize public places by removing the unwanted.[194] Racial and ethnic profiling by the police is a recurring source of concern,[195] yet PPVSS enhance police reliance on visually observable traits and actions to determine how to direct their attention.[196] The heightened importance of visual observation, to the exclusion of other sensory inputs, seems destined to exacerbate bias or the appearance of bias.[197] The potent combination of a technology that focuses exclusively on visible traits and allows the exacting attention of the police to take place at physical remove creates unique opportunities for targeting based on

191. *See supra* note 130. If, based on the totality of circumstances, the officer has a "suspicion that the particular individual being stopped is engaged in wrongdoing," he may stop the suspect, without a warrant, and frisk the suspect to search for weapons. United States v. Cortez, 449 U.S. 411, 418 (1981). The process of determining whether there is sufficient suspicion to justify a *Terry* stop "does not deal with hard certainties, but with probabilities," and should be understood from the officer's point of view: "the evidence . . . collected must be seen and weighed not in terms of library analysis by scholars, but as understood by those versed in the field of law enforcement." *Id.* For a comprehensive assessment of *Terry v. Ohio* by a wide variety of commentators, see *Terry v. Ohio 30 Years Later*, *supra* note 130.

192. *See* Lide, *supra* note 189, at 478–79.

193. *See id.*

194. *See* Lomell, *supra* note 150, at 351–55. *See generally* Koskela, *supra* note 153, 300–02 (examining the theory of power behind surveillance and exclusion). Researchers have also examined the way in which the focus on the visual downplays crimes that confound visually based identification—such as verbal harassment. *See* Koskela, *supra* note 69, 244–47.

195. *See* Samuel R. Gross & Debra Livingston, *Racial Profiling Under Attack*, 102 COLUM. L. REV. 1413, 1416–21 (2002).

196. *See* Lomell, *supra* note 150, at 354.

197. *See id.* at 359.

race, gender, ethnicity, and other protected classifications.[198]

d. Undermining Community Participation

The reduction in transparency at multiple levels, discussed above, decreases the opportunities for community participation and oversight in police practices. As more sophisticated systems come into use, the ability of the community to understand how they work and the implications of their use is further diminished.[199]

IV. REDUCING THE TENSIONS BETWEEN SURVEILLANCE AND DEMOCRACY

Viewing the challenges PPVSS pose to traditional mechanisms used to balance the tension between robust policing and the freedom from unchecked government power provides a constructive framework for considering possible responses. Responses to the power shifts caused by the introduction of PPVSS can be addressed through legal and procedural as well as technical measures. This Part first examines the approach San Francisco has taken with its Community Safety Camera Program that provides a current instantiation of such limits manifest in legal, procedural, and technical measures. Next this Article considers how a more flexible sensor-network—a network comprised of various sensing technologies rather than exclusively visual sensors—combined with a more thoughtful approach to front-end processing and data retention could assist in further reducing the concerns described above.

A. THE SAN FRANCISCO COMMUNITY SAFETY CAMERA PROGRAM

In 2005, with just two cameras, the San Francisco Mayor's Office of Criminal Justice launched the Community Safety Camera pilot program (CSC).[201] From its inception, the CSC was met with a mix of enthusiasm,[202] apprehension[203] and criti-

198. *See id.* at 347.

199. *See* SHAW, *supra* note 146, at 8.

201. Other camera systems operate within the city. This article considers only the CSC program for several reasons: 1) it is the only one which operates under an ordinance; 2) it is the one that prompted a sustained public discussion about surveillance cameras in the city; and, 3) one of the authors has detailed knowledge of the program having been the co-Principal Investigator on a six month review of the programs efficacy and effects required under the ordinance. CITRIS REPORT, *supra* note 42, at 7–9. *See id.*

202. *Id.* at 34 ("We need to make sure if this system is in place that it is effective in helping solve crime. . . . [T]he SFPD needs every tool they can get

cism.[204] The structure of the San Francisco CSC program is unique. The ambivalence of the community and the range of perspectives about the utility and desirability of the CSC program shaped the program in interesting ways.[205] The technical and administrative decisions, ordinance, practices, and procedures reflect the city's dual desire to empower law enforcement with new tools while simultaneously safeguarding rights and freedoms.[206]

A comprehensive review of the program undertaken by University of California at Berkeley investigators affiliated with the Center for Information Technology Research in the Interest of Society (CITRIS) in 2008 provides a detailed systems perspective on the CSC program.[207] In addition to analyzing crime reports to assess whether the CSC deterred any categories of crime or assisted in criminal investigation and prosecution, the drafters engaged in extensive data-gathering and analysis including: reviewing relevant legal codes and guidance documents published by the city; records of public hearings, contemporary news reports, press releases, and statements by the city and other stakeholders; the camera systems specifications, management, policies and procedures; and interviewing program stakeholders and end-users.[208]

To frame their analysis of the systems efficacy and effects the researchers first sought to document the goals that motivated its implementation.[209] Through a detailed review of public records, press statements, interviews with stakeholders, analy-

to help reduce the homicide rate and help reduce violent crime in the City." (quoting San Francisco Police Commission President Teresa Sparks)).

203. Jeff Adachi, Commentary, *Community, Not Just Technology, Needed in Crime Prevention*, S.F. CHRON., Sept. 13, 2006, at B11 ("Policies governing access to evidence from the cameras also should be crafted to protect the innocent as well as to prosecute the guilty.").

204. Rachel Gordon, *Mayor Wants Additional Surveillance Cameras*, S.F. CHRON., Oct. 24, 2005, at B6 (reporting that the American Civil Liberties Union (ACLU) views high-tech cameras as "sacrific[ing] precious privacy while providing very little in return in the way of added safety.") The ACLU "lamented" that San Francisco joined Chicago, New York City, and other municipalities, as "the latest city to succumb to the siren song of Big Brother technology." *Id*.

205. *See* CITRIS REPORT, *supra* note 42, at 33–34.

206. *Id*. at 42.

207. *See id*. at 33–34.

208. *See id*. at 47–50. In addition, the investigators conducted site visits to the cities of Los Angeles and Chicago for comparative approaches. *See id*. at 88.

209. *Id*. at 30–31.

sis of the system including policies and procedures, and the governing ordinance, the researchers identified two primary goals and a cluster of related secondary goals.[210] First, the deterrence of crime, specifically violent crime, was at the core of the city's mission.[211] Second and directly related, the city believed the system would provide additional evidence for prosecuting crimes.[212] These two primary goals were ringed by a set of secondary goals including community participation, accountability and oversight, and protection of privacy, freedom of expression, and related rights.[213] The analysis of the system considered the effectiveness of the system in relation to its primary goals—assessing its impact on crime and its utility in prosecution—and considered its effectiveness at protecting the secondary values articulated during the debates about the system and reflected in its design and regulation.[214] The detailed analysis of the relationship between the technical design, ordinance, policies, and practices of the CSC program and the secondary values provides long-overdue structure to these values in a particular system. For our purpose, the components of the system designed to protect the secondary values illustrate the primacy placed on transparency, limits on police discretion, community participation, and checks against bias. This design affirms Part III's assessment that considering PPVSS through the lens of criminal procedure and limitations on police practices generally provides a more fruitful approach than one based in privacy alone.

The structure of the San Francisco CSC program is unique in several respects. Below we discuss the technical capabilities, operational structure, and underlying policies, where appropriate comparing them to those adopted by other major cities. We then examine the policies reflect and support the secondary goals of community participation, accountability and oversight, and protection of privacy, freedom of expression, and related rights, and the mechanisms used to do so.

1. Technical Capabilities

The CSC program consists of seventy-one cameras.[215] Each

210. *See id*. at 36–42.
211. *Id*. at 33.
212. *Id*. at 35.
213. *Id*. at 36.
214. *See id*. at 26–30.
215. *Id*. at 170–71.

camera is connected[216] to a base station. The cameras compress and forward video, over a wired connection, for storage and later retrieval under a controlled set of circumstances.[217] The Department of Emergency Management (DEM) is in possession of the server and largely responsible for mediating access to its records consistent with the ordinance.[218] Although some of the cameras in the CSC program are Pan-Tilt-Zoom (PTZ cameras), the system is set up as a passive receptor of information.[219] There is no real-time access to footage.[220] This is quite distinct from cities like Chicago and New York which have opted for monitored systems based upon PZT cameras, and at times even mobile, cameras.[221] The CSC system is a standalone system.[222] It is not integrated into, or coordinated with, the City's 911 dispatch call system or other operational systems.[223] While other public and private camera system are in place in San Francisco, none of them feed data into the CSC server held by DEM; in general, users of those systems (transit authorities, shopkeepers, banks) may not access information maintained by DEM for the CSC program.[224] To date, San Francisco has not integrated the CSC program with other systems such as license plate readers[225] or additional sensing technologies such as shotspotters.[226]

In contrast, both the cities of Chicago and New York[227]

216. This connection may be wired or wireless. *Id*.

217. *See id*. at 174.

218. *See id*. at 97.

219. *See id*. at 171.

220. *See id*. at 178.

221. *See id*. at 181–82.

222. *See id*. at 170–71.

223. *See id*. at 178.

224. *Id*. at 97.

225. *Id*. at 100. Police investigators make use of footage from all city systems when investigating crime reports; however, there has been no effort to integrate the systems at the technical or operational level. *Id*. at 126.

226. *See* Jaxon Van Derbeken, *Early Gunshot Alert Little Help in Slaying*, S.F. CHRON., Jan. 28, 2009, at B2. San Francisco installed a $600,000 shotspotter system that uses sensors to triangulate the location of gunfire, but, although there were cameras in the area where a shooting occurred, the cameras did not record anything of use to investigators. *Id*.

227. The New York City surveillance system, which includes the Lower Manhattan Security Initiative (proposed in 2005, deployed in 2007), a proposed Midtown project (proposed 2009), the Metropolitan Transit Authority (MTA) system (proposed, but still in process), consists of public and private cameras, video and image analytics, and stationary as well as mobile devices. Al Baker, *Police Seek a Second Zone of High Security in the City*, N.Y. TIMES,

have systems that support real-time monitoring,[228] integrate video from public and private cameras,[229] and integrate data from other sensors and systems.[230] In Chicago, "[d]ispatchers will be able to tilt or zoom the cameras, some of which magnify images up to 400 times, in order to watch suspicious people and follow them from one range to anothers."[231] The New York system "include[s] not only license plate readers but also 3,000 public and private security cameras below Canal Street, as well as a center staffed by the police and private security officers . . . ."[232] The system is being integrated with new cameras that are "fully networked, with video-intelligence algorithms that aim to spot potential attackers."[233]

2. Operational Structure

The operational structure and management of the CSC program is, to the best of our knowledge, unique. Typically surveillance cameras used by the police are run and managed by the police department. For example, the Office of Emergency

Mar. 31, 2009, at A24. "[T]he Midtown zone would have at its core the collection of data, including license plate numbers and video of people on the streets. It would rely on a web of public and private security cameras feeding to a joint coordination center at 55 Broadway that became functional last fall." *Id*.

228. Even where technically possible, real-time monitoring of all cameras by individuals is unlikely to be the norm. While Chicago hopes to use other technology to enhance the effect of video surveillance by "creating something that knows no fatigue, no boredom and is absolutely focused," the reality today is that human limits are a constraint on the real-time, all-seeing Big Brother. City of Chicago, Firetide Wireless Mesh Key to City-Wide Video Security Deployment, http://www.firetide.com/innerContent.aspx?taxid=6&id=1140 (last visited Feb. 15, 2010).

229. Chicago links about 3000 city-operated cameras and cameras of more than 100 private companies. Daniel Schorn, *We're Watching: How Chicago Authorities Keep an Eye on the City*, CBS NEWS, Sept. 6, 2006, *available at* http://www.cbsnews.com/stories/2006/09/05/five_years/main1968121.shtml.

230. "License plate recognition, trending projections and intelligent search capabilities" will reportedly be integrated into the existing system in order to provide the ability to automatically identify suspicious behavior and issues alerts. Press Release, IBM, The City of Chicago's OEMC and IBM Launch Advanced Video Surveillance System (Sept. 27, 2007), *available at* http://www.03.ibm.com/press/us/en/pressrelease/22385.wss.

231. Stephen Kinzer, *Chicago Moving to 'Smart' Surveillance Cameras*, N.Y. TIMES, Sept. 21, 2004, at A18.

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

233. Noah Shachtman, *NYC is Getting a New High-Tech Defense Perimeter: Let's Hope It Works*, WIRED, Apr. 21, 2008, *available at* http://www.wired.com/politics/security/magazine/16-05/ff_manhattansecurity.

Management and Communications (OEMC), which coordinates emergency response of police, fire, emergency medical services, 911 services, and 311 city services, manages and operates the surveillance system in Chicago.[234] The New York City surveillance system is overseen and managed by the NYPD.[235] In contrast, San Francisco's CSC program was initiated by the Mayor's Office of Criminal Justice (MOCJ), and built by the Department of Telecommunications and Information Services (DTIS).[236] The CSC footage is placed in the custody of DEM.[237] The CSC program, as a result, has a fragmented operational structure in which DTIS has the sole ability to position and orient the cameras and the responsibility for system maintenance, the San Francisco Police Commission controls the placement of cameras subject to procedural requirements set out in the CSC Ordinance,[238] and DEM has custody and control over the footage subject to access and other provisions set out under the CSC Ordinance.[239] The CSC is not run or managed by the San Francisco Police Department (SFPD), and the CITRIS study found little interaction, beyond the retrieval of footage by investigators, between the police and the CSC program.[240] While the police, particularly police investigators, were conceived of as core users of the system, the technical and administrative composition of the system, together with the policies and procedures enacted to govern it, treat the police like third parties when it comes to accessing and using the system and footage.[241] The novel technical and administrative structure of the CSC program present challenges to integration with the SFPD's policing strategies; however, the structure is leveraged by the CSC Ordinance to support oversight and accountability

234. *See* Office of Emergency Management and Communications Homepage, http://egov.cityofchicago.org/oemc/ (last visited Mar. 11, 2010).

235. *See* Noah Shachtman, *The Shield*, WIRED, May, 2008, at 144, *available at* http://www.wired.com/politics/security/magazine/16-05/ff_manhattansecurity.

236. *See* CITRIS REPORT, *supra* note 42, at 28, 123.

237. *See id.* at 39.

238. The director of the MOCJ may recommend the installation of additional cameras to the Police Commission, which must then seek community input and engage in fact-finding and analysis prior to approving or denying an installation. *See id.* at 37–38.

239. *See id.* at 39.

240. *See id.* at 28–29 (discussing the limited input police had in camera placement and positioning and lack of policies about police interaction with DTIS for purposes of repositioning or addressing problems).

241. *See id.* at 13, 39–40.

for CSC program use consistent with its policy requirements.[242]

3. Policy

Mayor Newsom, the driving force behind the CSC program, began the public discussion by distancing himself and San Francisco's program from the video surveillance system in Chicago and proactively discussing limits on the system to address privacy and other concerns.[243] The City Board of Supervisors expressed mixed views on the system.[244] The Board of Supervisors passed the first version of the CSC Ordinance,[245] however, and they allowed the City to expand the number of cameras.[246]

The CSC Ordinance is a highly instructive artifact. Its provisions provide a clear sense of the privacy and other risks legislators and the public associate with video surveillance systems.[247] Several sets of guidelines for public video surveillance systems have been published in recent years[248] however the

242. *See id*. at 30–42.

243. *See* Rachel Gordon, *Mayor Wants Additional Surveillance Cameras*, S.F. CHRON., Oct. 24, 2005, *available at* http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2005/10/24/BAGA0FCQQ91.DTL (discussing prohibitions on pointing CSC cameras inside people's homes or at residential doorways promised by Mayor Newsom). Before the system was rolled out a spokesman for the Mayor sought to assuage the concerns of the ACLU and others on National Public Radio stating that, "[t]hey'll record only images, not sound, for 72 hours. After that, the digital recordings are automatically erased unless the Police Department wants to see them. The cameras will not be monitored." Richard Gonzales, *All Things Considered: San Francisco Considers Video Surveillance*, (NPR broadcast Nov. 4, 2005) *available at* http://www.npr.org/templates/story/story.php?storyId=4990088&ps=rs.

244. *See* CITRIS REPORT, *supra* note 42, at 36.

245. *See* S.F., CAL., ORDINANCE 127-06 (June 6, 2006) *available at* http://www.sfgov.org/site/uploadedfiles/bdsupvrs/ordinances06/o0127-06.pdf (amending S.F. ADMIN. CODE ch. 19, §§ 1–8 (2006)).

246. *See* Demian Bulwa, *Police Commission OKs More Cameras—25 at 8 Locations*, S.F. CHRON., Jan. 18, 2007, at B3.

247. *See* S.F., CAL., ORDINANCE 127-06.

248. For examples, see DEP'T HOMELAND SEC., PRIVACY OFFICE PUBLIC WORKSHOP, CCTV: DEVELOPING BEST PRACTICES, (Dec.18, 2007) (transcript), *available at* http://www.dhs.gov/files/publications/editorial_0514.shtm; OFFICE OF THE PRIVACY COMM. OF CAN., GUIDELINES FOR THE USE OF VIDEO SURVEILLANCE OF PUBLIC PLACES BY POLICE AND LAW ENFORCEMENT AUTHORITIES (Mar. 2006), *available at* http://www.privcom.gc.ca/information/guide/vs_060301_e.asp; GOV'T OF B.C., PRIVACY GUIDELINES FOR USE OF VIDEO SURVEILLANCE TECHNOLOGY BY PUBLIC BODIES (2004), *available at* http://www.lcs.gov.bc.ca/privacyaccess/main/video_security.htm; OFFICE OF THE INFO. & PRIVACY COMM. FOR B.C., PUBLIC SURVEILLANCE SYSTEM PRIVACY GUIDELINES (Jan. 26, 2001), *available at* http://www.oipcbc.org/advice/VID-SURV(2006).pdf; INFO. & PRIVACY COMM. OF ONT., GUIDELINES FOR USING VIDEO SURVEILLANCE CAMERAS IN PUBLIC PLACES (Sept. 2007), *available at*

CSC Ordinance is one of the only regulatory frameworks governing a permanent public video surveillance system in the United States.[249] The regulatory oversight and enforcement is a singularly striking aspect of the CSC program.[250]

The CSC Ordinance responded to concerns that the program would undermine civil liberties, civil rights, and privacy. These amorphous high-level concerns led the San Francisco Board of Supervisors to direct the city attorney to draft legislation instituting enforceable guidelines to ensure that constitutional rights were not abused or compromised as a result of the operation of the CSC program.[251] The city attorney chose decidedly more pragmatic language to describe the aims of the CSC ordinance: "to regulate the installation of community safety cameras, prescribe a notification and approval process for the installation of cameras, and to establish protocols for oversight and access to video recordings."[252] While the language is primarily process-oriented, the structure of the CSC Ordinance taken as a whole manifests the Board's goals of facilitating community participation, limiting law enforcement discretion over system use, ensuring accountability and oversight over both system use and system effectiveness through transparen-

http://www.ipc.on.ca/images/Resources/up-video_e.pdf; THE CONSTITUTION PROJECT, *supra* note 65; ELEC. PRIVACY INFO. CTR., PROPOSED PRIVACY CONDITIONS FOR VIDEO SURVEILLANCE (Jan. 15, 2008), *available at* http://epic.org/privacy/surveillance/epic_cctv_011508.pdf.

249. Washington, DC regulates the use of video surveillance by the Metropolitan Police Department. *See* D.C. MUN. REGS. tit. 24, § 1 (2002). The Fresno City Council approved a policy manual to govern the Police Department's use of video surveillance system as a condition of releasing $1.2 million in program funding. *See* Mike Rhodes, *Video Surveillance Project Gets Final Approval*, CENTRAL VALLEY, Aug. 22, 2006, http://www.indybay.org/newsitems/2006/08/22/18299898.php (last visited Mar. 11, 2010).

250. Many nonprofit organizations and scholars that have raised concerns about the proliferation of video surveillance cameras across the country have been specifically disturbed by the lack of public input and regulation of the programs. *See* SCHLOSBERG & OZER, *supra* note 25, at 16 (discussing the lack of enforceable regulations and lack of policies guiding such systems in California, with the exception of San Francisco as of June 2006); THE CONSTITUTION PROJECT, *supra* note 65, at 20–21 (recommending public oversight and accountability through "a detailed, participatory and transparent process" in which "members of the community that would be affected by a proposed system [] have the opportunity to participate in the decision to create such a system, as well as the subsequent major decisions affecting its coverage and capabilities").

251. City of San Francisco Board of Supervisors Meeting, Nov. 15, 2005, *available at* http://www.sfgov.org/site/uploadedfiles/bdsupvrs/minutes/m111505.htm.

252. S.F., CAL. ORDINANCE 127-06.

cy-forcing provisions, and protecting privacy, civil liberties, and civil rights.[253]

a. Community Participation

A commitment to community participation is found in provisions requiring public discussion about the expansion of CSC program and a requirement that significant support from the affected community exist for a proposed camera installation.[254] It is the only public surveillance camera program that requires the concerns of the affected community to be considered in decisions about whether to install cameras in specific places, or to require the support of the affected community for such an installation.[255] CSC provides both pre-installation notice[256] to facilitate community participation in the decision of whether to install CSC program cameras, and post-installation notice (through the placement of cameras and signs) of the areas under surveillance.[257] The "affected community"—left undefined but apparently meant to include people who live and/or own property within the camera's field of view[258]—is a privileged player in the deliberation about whether to approve the instal-

253. *See* CITRIS REPORT, *supra* note 42, at 33–40.

254. S.F., CAL., ADMIN. CODE § 19.4(c) (2006) (requiring the Police Commission to weigh "any concerns asserted by the affected community" against the potential of the proposed camera installation to deter criminal activity, and allowing an installation to be approved if there is "significant support from the affected community for the camera").

255. CITRIS REPORT, *supra* note 42, at 113. Washington, DC requires that public notice of proposed camera installations be provided and the public be guaranteed thirty days to submit comments that the police chief must consider and then provide an explanation of the decision to install, or not install, cameras. *Id*.

256. *See* S.F., CAL., ADMIN. CODE § 19.5(b)(1)–(3) (2006).

257. *Id*. § 19.2 (requiring the cameras to be installed "at fixed locations in an open and obvious manner"); *id*. § 19.5(c) (requiring a "conspicuous" sign to be placed within twenty-five feet of the new camera or cameras, notifying the public that the area is under surveillance and requiring "the location of all [CSC program] cameras installed throughout the City" to be posted on the SFPD web site).

258. The term "affected community" is not defined in the ordinance. *See id*. However, a provision that allows MOCJ, at its discretion, to provide additional notice through mailed notices of a proposed installation sheds some light on the meaning of affected community. *Id*. § 19.5(b)(1)–(3). If MOCJ provides mailed notices, it is required to send them to "(1) The owner of each property within 300 feet of the proposed camera location . . . (2) Neighborhood associations and organizations . . . within 300 feet of the proposed camera location, and (3) . . . occupants of each property within 300 feet of the proposed camera location." *Id*.

lation of CSC cameras in a given neighborhood.[259]

b. Limiting Police Discretion

Numerous provisions of the ordinance, in addition to the technical and operational structure discussed above, constrain law enforcement access and use of the system.[260] While the MOCJ proposes, based on crime statistics, where to locate cameras, as discussed above, the final decision about whether to install cameras is made after community input and with community support by a decision of the Board.[261] Resting control over camera locations with the elected body establishes a baseline for oversight of the CSC program. CSC cameras, according to the ordinance, can only record "areas perceptible to the human eye from public streets and sidewalks."[262] While the police department has input into the positioning of cameras, the final arbiter of placement is the Board.[263] The CSC program, compared to other video surveillance systems, wrests discretion about its deployment and use from the police, and subjects it to debate and deliberation in a legislative forum.[264] The decisions about camera placement made by the publicly elected officials are further constrained by substantive and procedural rules that demand deference to the concerns of the affected community.[265]

The CSC program, both cameras and footage, is in the hands of entities other than the SFPD: DTIS and DEM respectively.[266] This structure is used to manage access and use of the

259. *Id*.

260. *See* CITRIS REPORT, *supra* note 42, at 97–100.

261. *See* S.F., CAL., ADMIN. CODE § 19.4(a) (requiring the director of MOCJ only to make a recommendation to the Police Commission to install cameras where he or she finds "that a particular location is experiencing substantial crime and that the potential to deter criminal activity outweighs any concerns asserted by the affected community"); *id*. § 19.4(b) (requiring the Police Commission to hold a public hearing about the proposed camera installation, and to weigh "any concerns asserted by the affected community" against the potential of the proposed camera installation to deter criminal activity, and limiting installation to where there is "significant support from the affected community for the camera"). The MOCJ report must be distributed to the Police Commission and the public "20 days prior to the first public hearing on the proposed installation." *Id*.

262. *Id*. § 19.3.

263. *See id*. § 19.4(d).

264. *See id*. § 19.4(b).

265. *See supra* Part IV.A.3.i.

266. CITRIS REPORT, *supra* note 42, at 39.

video footage.[267] Specifically, it removes questions about how law enforcement can best use the CSC program footage, supplanting it with the Board's determinations on legitimate uses.[268] Initially the CSC Ordinance had no provisions for access by anyone except law enforcement.[269] It was subsequently amended to provide for access by defense counsel where a charge has been lodged, and limits the use of the footage to the defense of that charged criminal case.[270] Police investigators may only obtain copies of CSC program footage for investigation of specific crimes and defense counsel may only obtain it for investigating charged cases.[271] Under the CSC Ordinance police are granted no other specific means to access CSC program footage.[272] They may not routinely view it and they may not access it unless they are investigating a specific crime.[273] Requests for CSC program footage must be documented in writing[274] and DEM is responsible for ensuring that footage is released in accordance with the statute.[275]

c. Transparency, Oversight and Accountability

The CSC Ordinance creates a nearly complete and auditable record of the CSC program's use[276] and structure. However,

267. *See id*.

268. S.F., CAL., ADMIN. CODE § 19.3 ("Images obtained by the community safety cameras may be released only to the following: (a) Sworn members of the San Francisco Police Department holding the rank of Inspector or higher. Police shall limit review of images to investigation of specific crimes . . . .").

269. *See* CITRIS REPORT, *supra* note 42, at 102–06.

270. S.F., CAL., ADMIN. CODE § 19.6(c)(2).

271. *See id*. § 19.6(c).

272. The Ordinance does not explicitly prohibit SFPD from viewing the footage at DEM, but the structure suggests that section 19.6(b) is designed to constrain all access to CSC program footage. *See id*. § 19.6(b). Section 19.3(a) limits "review" of footage to SFPD rank of inspector or higher and for the purpose of investigating specific crimes. *See id*. § 19.3(a). Section 19.6(b) limits how SFPD inspectors can obtain "copies" of CSC program footage, and provides an exigent circumstances exception that allows the filing of the forms and approval to occur after DEM has "released" the footage to them. *See id*. § 19.6(b). The inconsistent and overlapping terms in the ordinance create some ambiguity.

273. *See id*. §§ 19.3, 19.6.

274. *Id*. § 19.6(c). There is an exigent circumstances exception but it to requires a subsequent written request to be filed. *Id*.

275. *Id*. § 19.6(a) ("DEM staff shall be responsible for proper release of the records.").

276. The lack of resources at DEM combined with a desire to avoid needless requests to copy footage resulted in some police investigators reviewing footage, at the DEM office, for a particular time and date prior to making a

the CSC Ordinance goes further, requiring the SFPD to prepare an annual report to the city Board of Supervisors and the Police Commission that includes the:

> camera locations, the crime statistics for the vicinity surrounding each camera both before and after the camera is installed, crime statistics from surrounding vicinities, the number of times the Police Department requested copies of the recorded images, the number of times the images were used to bring criminal charges, the types of charges brought, and the results of the charges.[277]

San Francisco is unique among U.S. cities in requiring this information to be collected and provided to an external oversight body that may then act on it, ordering the removal of any individual camera.[278] Through this mix of recordkeeping and reporting requirements, the CSC Ordinance makes the use and operation of the CSC system transparent and creates a record for the Board and the public to periodically assess the utility and desirability of the system, as well as audit for its misuse.[279]

B. NETWORKS OF MULTIPLE SENSORS CAN FURTHER REDUCE TENSIONS BETWEEN POLICING AND DEMOCRACY

Advances in technology present a double-edged sword: advanced sensing increases the potential for covert surveillance of increased acuity, but distributed processing, remote computational capabilities, and the ubiquitous cellular platform have increased the potential for transparency and selectively limiting what is actually captured by sensing platforms. "Although it may seem counterintuitive, improved surveillance technology could actually help to increase individual privacy in the future in two ways: by allowing for more refined and less intrusive searches, and by increasing the monitoring of law enforcement."[280]

---

request for a copy of that footage—and in some instances it is unclear whether such access was subsequently documented. *See* CITRIS REPORT, *supra* note 42, at 98. For this reason, we must accept that the record of system use contains some gaps.

277. S.F., CAL., ADMIN. CODE § 19.4(d). A resolution passed in 2008 authorized the CITRIS evaluation to stand in for the SFPD's report. S.F., Cal., Board of Supervisors Resolution 71-08 (Feb. 5, 2008), *available at* http://www.sfgov.org/site/uploadedfiles/bdsupvrs/resolutions08/r0071-08.pdf (extending deadline for report to March 20, 2008, and recognizing CITRIS's participation in the report's production).

278. *See* S.F., CAL., ADMIN. CODE § 19.4(d).

279. *See* CITRIS REPORT, *supra* note 42, at 39–40, 114–17.

280. Ric Simmons, *Why 2007 Is Not Like 1984: A Broader Perspective on Technology's Effect on Privacy and Fourth Amendment Jurisprudence*, 97 J. CRIM. L. & CRIMINOLOGY 531, 563 (2006).

Transparency is equity—the watchers and the watched have a common understanding as to what data is being collected. The simplest example of surveillance transparency is the red light that adorns many video cameras. When the light is on, one is to understand that the camera is on as well. Along with such visual notifications, new technologies provide the potential for greater transparency. The cellular platform, for example, offers a unique basis for notification—it is possible to provide text warnings to cell phones within a limited distance of a surveilled area.[281] The text message could be required by regulation, and would specify exactly what data is being collected. Given the ubiquity of cellular phones and the flexibility of texting, the cellular platform can play a significant role in transparency if service providers are willing.

Technology can also play a role in limiting the downsides of the human factor. User discretion is a significant problem with many surveillance technologies;[282] a surveillance system may be deployed for a publicly stated purpose, and later used for other purposes based solely on the discretion of local law enforcement. Surveillance may also be abused for purely personal reasons. In one of many examples, in 2003 a traffic camera in Tuscaloosa, Alabama, was seen panning and zooming in an apparent effort to track young women.[283] The camera was controlled by the Alabama State Troopers Office and was intended solely for traffic support, but according to the Associated Press, the camera had been taken over to monitor potential criminal activity.[284] In another example, in 2006, two CCTV operators in Merseyside, England were jailed for spying on a woman in her own home.[285] Many other examples could be provided; there is a clear need for limiting operator discretion.

Highly specific sensing technologies offer one means of li-

281. This type of notification system has been used with weather warnings. *See* Ryan Loew, *Lansing to Launch New Text-Messaging Alert Service*, LANSING ST. J., Nov. 16, 2009.

282. *See, e.g.*, Slobogin, *supra* note 49, at 248–50.

283. Jon Gagis, *Strip Traffic Camera Follows Pedestrians*, THE CRIMSON WHITE, Sept. 15, 2003, *available at* http://www.cw.ua.edu/2.4648/strip-traffic-camera-follows-pedestrians-1.1220008.

284. The Surveillance Camera Players, *A Sarcastic Open Letter Dated 17 September 2003 and Addressed to All Those Involved in or Ultimately Responsible for the Recent Scandal Involving Egregious Abuses of a Government Surveillance Camera in Tuscaloosa, Alabama*, NOT BORED!, http://www.notbored.org/tuscaloosa.html.

285. *Peeping Tom CCTV Workers Jailed*, BBC NEWS, Jan. 13, 2006, http://news.bbc.co.uk/2/hi/uk_news/england/merseyside/4609746.stm.

miting discretion, as they limit the extent to which collateral data is collected. Any sensing technology can be made more specific, focusing on particular patterns through the use of signal processing.[286] For example, a nonspecific audio sensor will collect any detectable audio signal within a certain bandwidth; voice, music, and personal interaction are all captured without regard to the actual target of the surveillance. A pattern-specific audio sensor, on the other hand, will look for audio signatures that fit a particular voice, a particular sound, or even a particular set of words, while rejecting (and not recording) other inputs.[287] Gunshot sensors provide an excellent example. Washington, D.C. police are currently using ShotSpotter, a network of noise sensors that identifies and pinpoints gunfire, to detect shooting incidents.[288] This technology allows for law enforcement response well before a 911 call can be placed.[289] According to the manufacturer, the sensors are so sensitive that they can distinguish between gunfire and such sounds as firecrackers and car backfires.[290] Originally developed to monitor earthquakes, the technology uses acoustic software to detect urban gunfire.[291]

As a variation on this theme, personally identifiable traits can be isolated and removed from video and audio surveillance data through advanced pattern recognition algorithms. For example, it is possible to automatically filter facial information from a video data stream.[292]

Automated sensing provides another means for reducing the discretion of law enforcement. Adaptive algorithms have

286. *See* Robert Collins, *Algorithms for Cooperative Multisensor Surveillance*, 89 PROCEEDINGS OF THE IEEE 1456, 1456 (2001).

287. *See* Yaniv Zigel, *A Method for Automatic Fall Detection of Elderly People Using Floor Vibrations and Sound—Proof of Concept on Human Mimicking Doll Falls*, 56 IEEE TRANSACTIONS ON BIOMEDICAL ENGINEERING 2858, 2859 (2009).

288. *See* ShotSpotter, http://www.shotspotter.com (last visited Mar. 11, 2010); *see also* Carol Leonnig, *Noise Sensors Back Police on Shooting of D.C. Teen*, WASH. POST, Oct. 31, 2007, at A01.

289. *See* Allison Klein, *Gunshot Sensors are Giving D.C. Police Jump on Suspects*, WASH. POST.COM, Oct. 22, 2006, http://www.washingtonpost.com/wp-dyn/content/article/2006/10/21/AR2006102100826.html.

290. ShotSpotter Overview, http://www.shotspotter.com/solutions/index.html (last visited Mar. 11, 2010).

291. *See* Klein, *supra* note 289.

292. *See* Rein-Lien Hsu, *Face Detection in Color Images*, 24 IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE 696, 696–07 (2005).

made possible cooperative multisensor platforms that require the support of a single officer.[293] Advanced algorithmic techniques have also made possible fully automated facial recognition[294] and analysis,[295] eliminating the need, in many instances, for any active video monitoring by law enforcement personnel.

CONCLUSION

We are sliding towards a surveillance society.[296] Technological advances that will enable the government to engage in increasingly invisible, yet exacting, surveillance are on the horizon. If current trends continue a growing number of communities around the country will willingly embrace—albeit with little consideration of its relative costs and benefits—visual surveillance systems for public spaces. As justices and judges have signaled, such a decision raises profound questions of how to maintain the checks and balances, that preserve freedoms and liberties, while supporting robust policing on law enforcement power, reflected in criminal procedure and police oversight structures.

While the courts may be institutionally constrained in their ability to consider the impending 24/7 surveillance state, the legislature and executive branches are not. The introduction of permanent video surveillance systems into public places should be the product of a robust debate. Such systems, like other law enforcement investigative tools, should be accompa-

293. *See* Collins, *supra* note 286, at 1456.

294. Mao Wei & Abbas Bigdeli, *Implementation of a Real-Time Automated Face Recognition System for Portable Devices*, 1 INT'L SYMP. ON COMM. & INFO. TECH. 89, 89 (2004).

295. Jeffrey F. Cohn & Takeo Kanade, *Automated Facial Image Analysis for Measurement of Emotion Expression*, *in* THE HANDBOOK OF EMOTION ELICITATION AND ASSESSMENT 222, 222 (J. A. Coan & J. B. Allen eds., 2007).

296. Scholars from a variety of disciplines claim that we long ago arrived, however we believe that a society under round-the-clock video surveillance, when in public places, is qualitatively different then the piecemeal surveillance we experience yet today. We still have time to reconcile video surveillance and other sensing technologies with democratic values. It is not too late to take action. *See generally* DAVID FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES (1989) (examining the passage, revision, and implementation of data protection laws in five countries with a focus on efforts to control surveillance by officials); DAVID LYON, SURVEILLANCE SOCIETY (2001) (describing the relationship between technology and privacy while advocating an in-depth understanding of how surveillance reinforces division into social categories); CLIVE NORRIS & GARY ARMSTRONG, THE MAXIMUM SURVEILLANCE SOCIETY (1999) (describing the social and political trends revealed in the rush to install CCTV).

nied by checks and balances. These checks and balances should include technical measures and policies that make the deployment and use of video surveillance systems in public places transparent to the public, constrain law enforcement discretion, support community participation in the deployment and use of such systems, and limit bias in policing decisions.

To date Congress has been largely silent on our federally subsidized slide into surveillance.[297] Given the important role statutory privacy laws play in governing electronic surveillance[298] in other forms—providing more detailed rights and obligations than case law typically does—the federal government's role in funding the creation of a distributed public surveillance infrastructure, and the constraints on the judiciary to craft governing rules, Congress and the Administration should steward this effort. This Article has provided technical and policy recommendations to guide such efforts.

297. On Dec. 16, 2005, The House Committee on Homeland Security, Subcommittee on Management Integration and Oversight, held a hearing on the Integrated Surveillance Intelligence System (ISIS) on the U.S.-Mexico border. *Mismanagement of the Border Surveillance System and Lessons for the New Secure Border Initiative: Hearing Before the Subcomm. on Management, Integration, and Oversight of the H. Comm. on Homeland Security,* 109th Cong. 1 (2005) (statement of Richard L. Skinner, Inspector General, U.S. Department of Homeland Security). Richard L. Skinner, Inspector General of DHS testified that the remote video surveillance system already in place on the U.S.-Mexico border was ineffective and had fallen short of expectations. *Id.* at 2. In June 2003, the General Accounting Office released a report on video surveillance systems installed by the U.S. Park Police and the Metropolitan Police Department, noting that the Constitution Project found the police department's regulations for the use of CCTV "lacked clarity and specificity in some areas, such as training of CCTV operators." U.S. GEN. ACCOUNTING OFFICE, VIDEO SURVEILLANCE: INFORMATION ON LAW ENFORCEMENT'S USE OF CLOSED-CIRCUIT TELEVISION TO MONITOR SELECTED FEDERAL PROPERTY IN WASHINGTON, D.C. 4 (2003), *available at* http://www.gao.gov/new.items/d03748.pdf.

298. *See* Kerr, *supra* note 61, at 838.