SEEING PAST PRIVACY: WILL THE DEVELOPMENT AND APPLICATION OF CCTV AND OTHER VIDEO SECURITY TECHNOLOGY COMPROMISE AN ESSENTIAL CONSTITUTIONAL RIGHT IN A DEMOCRACY, OR WILL THE COURTS STRIKE A PROPER BALANCE?

Robert D. Bickel Susan Brinkley Wendy White ***

I.	INTR	ODUCTION	300
II.	HIST	ORY	301
III.	CONS	STITUTIONAL LAW AND PRIVACY	
	PRIN	CIPLES GOVERNING THE USE OF VIDEO	
	SECU	JRITY TECHNOLOGY	307
	A.	Federal Law	307
	B.	State Court Cases and State Privacy Law	316
	C.	Summary of Constitutional and Privacy Issue	es321
IV.	EMPI	LOYER USE OF VIDEO SURVEILLANCE	
	IN W	ORK AREAS	323
V.	TORT	CLAIMS AND VIDEO SURVEILLANCE	333
	A.	Negligence Principles	333
	B.	Application of Negligence Principles in the Co	ontext
		of Video Surveillance	337
		1. Failure to Utilize a Video Security	
		System	337
		-	

 $^{^{\}ast}$ © 2003, Robert D. Bickel. All rights reserved. B.A., University of South Florida; J.D., with highest honors, Florida State University; Professor of Law, Stetson University College of Law.

^{** © 2003,} Susan Brinkley. All rights reserved. B.A., *magna cum laude*, M.A., Memphis State University; Ph.D., Sam Houston State University; Associate Professor of Criminology, University of Tampa.

^{*** © 2003,} Wendy White. All rights reserved. A.B., magna cum laude, Phi Beta Kappa, Gaucher College; J.D., magna cum laude, University of Pennsylvania; Vice President and General Counsel, University of Pennsylvania and University of Pennsylvania Health System.

300			Stetson Law Review [Vol. XXXIII		
		2.	Use of Video Surveillance to			
			Replace Security Guards or Officer	rs 339		
		3.	Policies, Procedures, and Employe	e		
			Training	340		
		4.	False Sense of Security	340		
		5.	Governmental Immunity	341		
	C.	Inva	asion of Privacy and Infliction of Emot	ional		
		Dist	ress	342		
	D.	A Co	A Comparative Look at the United Kingdom:			
		Info	rming the United States' Perspective			
		of Co	345			
		1.	CCTV in City Centers	346		
		2.	Role of the European Union	347		
		3.	Criticisms about Lack of Privacy			
		4.	Legislative Response to Criticism.	349		
		5.	Privacy and the Police	351		
		6.	Regulations Governing Procedures	\$		
			and Practice of CCTV	360		
		7.	Summary	363		
VI.	CON	CLUS	ION			

I. INTRODUCTION¹

Privacy is not an absolute. It is contextual and subjective. It is neither inherently beneficial nor harmful. Rather, the term connotes a complex aggregation of positive and negative attributes.²

Legal dialogue among scholars in the fields of constitutional law and the commons law of privacy about the emerging applica-

^{1.} The Authors wish to thank Pamela D. Burdett, Research Librarian, Stetson University College of Law, and Leeanne L. Frazier, Research Assistant to Professor Bickel, for their work on this project and their contributions to this Article. This Article originated as a work in progress associated with a meeting of police, private security, and security industry representatives, sponsored by the Security Industry Association (SIA), in Washington in the Spring of 1999.

^{2.} Fred H. Cate, Privacy in the Information Age 31 (Bookings Instn. Press 1997); see Daniel Solove, Conceptualizing Privacy, 90 Cal. L. Rev. 1087, 1093 (2002). Professor Solove suggests that to discuss privacy in the abstract is to make a generalization about particular practices that are a product of history and culture. Id. at 1092-1093. He proposes that "we ... explore what it means for something to be private contextually by looking at particular practices. . . . [P]rivacy should be conceptualized contextually as it is implicated in particular problems." Id. at 1093.

301

tions of video security technology has been ongoing for more than a decade. Early articles on the constitutionality of using closed-circuit television (CCTV) technology for "citizen safety" purposes³ documented the first series of projects and raised fundamental constitutional issues that have been the subject of real outcomes described in the most recent legal commentary.⁴ In ten short years, the legal literature has drawn some fairly solid conclusions based upon both theory and experience. Recently, constitutional concerns for privacy have also been raised in the context of the emerging use of such technology by employers to monitor employees' suspected incriminating conduct that threatens the employer's economic interests.⁵

In the private law context, tort law has begun to examine the use of video security systems in two distinct areas. First, the courts have had to analyze, under negligence principles, the necessity of video surveillance in satisfying a landowner's duty—as landlord, school, commercial business, etc.—to take reasonable measures to deter criminal activity on the landowner's premises. Second, the courts have also had to grapple with the potential imposition of tort liability on landowners and others for "invasion of privacy" claims resulting from the installation and use of this same technology. The discussion that follows attempts to summarize this emerging dialogue, identify the most critical legal and policy issues, and focus the debate between privacy concerns and security interests that is occasioned by increased reliance on video surveillance technology in both the United States and the United Kingdom.

II. HISTORY

Commentator Quentin Burrows notes that video surveillance technology was introduced in certain cities in the United States as early as 1956 to assist police in reducing crime on public streets. Early projects included using video technology in Hobo-

^{3.} E.g. Jennifer M. Granholm, Video Surveillance on Public Streets: The Constitutionality of Invisible Citizen Searches, 64 U. Det. L. Rev. 687 (1987) (discussing video surveillance cameras placed on public streets to deter crime).

^{4.} See Quentin Burrows, Scowl Because You're on Candid Camera: Privacy and Video Surveillance, 31 Val. U. L. Rev. 1079, 1083 (1997) (discussing video surveillance and the competing values of safety and privacy).

^{5.} *Infra* pt. IV (discussing employer use of video surveillance).

^{6.} Burrows, supra n. 4, at 1080.

ken, New Jersey, in 1966, and in Mount Vernon, New York, in 1971. Both Burrows and Michigan Governor Jennifer Granholm describe these early projects as generally unsuccessful, and Burrows paints a similar picture of a later 1982 project in Dade County, Florida. Granholm adds that, while many citizens may have been willing to trade privacy for safety, and thus did not mind being watched, some officers were concerned that cameras would be used to monitor the police officer and that criminals would quickly learn to simply avoid areas within camera range. In spite of these early, unsuccessful efforts, subsequent projects followed in several states. Many of these projects were reasona-

^{7.} *Id.* at 1103. Burrows describes projects in Hoboken, New Jersey; Olean, New York; Mt. Vernon, New York; and Times Square. *Id.* He indicates that all of these first systems were dismantled when they were found to be ineffective or when they failed to produce significant numbers of convictions. *Id.* (citing Gary C. Robb, *Police Use of CCTV Surveillance: Constitutional Implications and Proposed Regulations*, 13 U. Mich. J.L. Reform 571, 572 (1980)).

^{8.} Granholm, *supra* n. 3, at 688. Granholm's article, inspired by the introduction of a significant video surveillance program in Detroit in 1986, describes the alleged failure of the early Hoboken and Mount Vernon projects. *Id.* at 687. Granholm notes that the Mount Vernon project produced no convictions, and the Hoboken project led to only one arrest in five years. *Id.* at 688.

^{9.} Burrows, *supra* n. 4, at 1082. The Dade County, Florida project, which local volunteers monitored on a twenty-four-hour basis, was discontinued in 1984 with no convictions. *Id.* Although the Dade County project planned to use police employees, the project instead used community employees, mostly elderly, and experienced significant equipment failure. *Id.*

^{10.} Id. at 1103 n. 183.

^{11.} Granholm, *supra* n. 3, at 688–689; *see e.g. Gross v. Taylor*, 1997 WL 535872 (E.D. Pa. Aug. 5, 1997) (concerning the interception of officers' private conversations in their patrol cars).

^{12.} Burrows, supra n. 4, at 1103-1106. Subsequent projects followed in Anchorage, Alaska (street surveillance cameras controlled by private residents); Baltimore, Maryland (cameras monitored by a cooperative effort between police and private citizens); Camden, New Jersey (street surveillance of Westfield Acres Housing Projects); Dover, New Jersey (cameras installed in 1993 to monitor the downtown area); South Orange, New Jersey (seven cameras monitored by police station personnel); Heightstown, New Jersey (cameras installed to monitor trouble spots in housing projects); Los Angeles, California (privately funded program using volunteers to monitor street surveillance cameras mounted on apartment buildings); Virginia Beach, Virginia (ten low-light-sensitive cameras on street light poles in busy beach areas); Kinston, North Carolina (twenty video cameras on utility poles monitored twenty-four hours a day); Memphis, Tennessee (ten operational cameras and plans to expand to seventy-two); San Diego, California (five cameras in Balboa Park); and Tampa, Florida (eight cameras allow police to monitor the busy Ybor City District). Id. For descriptions of the Ybor City project, see Richard Danielson, Smile, Ybor: You're on Crime Camera, St. Petersburg Times 1B (June 7, 1996) (available at 1996 WL 7119969), Richard Danielson, Police Cameras May Soon Scan Ybor, St. Petersburg Times 1B (May 24, 1996) (available at 1996 WL 7117611), and Ivan J. Hathaway, Decision Delayed on Video Surveillance in Ybor: Council Members Are Worried Videotaping Visitors to Ybor

bly successful in producing arrests and convictions, as well as reducing criminal activity; additionally, they could be managed in ways that minimized the risk of intrusive surveillance or taping.¹³

Burrows accurately describes the standards by which such projects should be evaluated: The use of CCTV and other video security technology must be effective in reducing crime and otherwise protecting citizens, including employers and employees, and, at the same time, the use of such technology must be subject to constitutional limitations, rules of private law, and protocols of ethics and professionalism, which prohibit unreasonable intrusion into the privacy rights of individuals.¹⁴

From these points of reference, the criticism of these projects, by both citizen-rights groups and political officials of both major national parties, is not that they fail to withstand constitutional challenge, but that they are costly and ineffective in bringing about arrests and convictions and that they add to the negative image of policing by creating a "big brother is watching you" environment on city streets and in places of public accommodation and employment.¹⁵ Privacy concerns are supported by cases as well as electronic media and newspaper accounts of (1) the rapid,

City May Violate Their Privacy, Tampa Trib. 1 (May 24, 1996) (available at 1996 WL 10228767).

^{13.} Burrows, supra n. 4, at 1122–1125. Among the cited examples of widely publicized successes are the following: the use of video surveillance to apprehend the suspects involved in the bombing of the Oklahoma City Federal Building; the "Bulger" case $(V.\ v.\ United\ Kingdom, 30$ Eur. H.R. Rep. 121 (2000)), in which video surveillance helped police apprehend two boys who murdered a two-year-old child; the thirty percent drop in crime in Boston housing projects; and significant arrests in Camden, New Jersey; Memphis, Tennessee; and Tacoma, Washington, as a result of the installation of video surveillance technology. Burrows, supra n. 4, at 1122–1125. Cities may discourage the unauthorized or abusive use of video surveillance by simply avoiding the use of tapes or by recycling them after a certain number of hours. Id. at 1124.

^{14.} See generally Burrows, supra n. 4 (discussing privacy and video surveillance).

^{15.} See generally Andrew E. Taslitz, The Fourth Amendment in the Twenty-First Century: Technology, Privacy and Human Emotions, 65 L. & Contemp. Probs. 125 (2002) (discussing privacy implications of video surveillance systems). As Taslitz notes, the "big brother" phrase is more than merely reminiscent of George Orwell's 1984—it captures the image of a society that engages in the "constant, state-initiated surveillance of its [citizens]." Id. at 125–126. In noting the reality of this imagery, Taslitz notes that, while so-called "smart CCTV" (face recognition technology) has potential military application, "We are taking a step in the wrong direction if we allow this powerful technology to be turned against citizens who have done no wrong." Id. at 126 (citing Dana Canedy, Tampa Scans the Faces of Its Crowds for Criminals, N.Y. Times A1 (July 4, 2001) (quoting House Majority leader Richard Armey)). Professor Daniel Solove notes that current conceptualizations of privacy include freedom from surveillance. Solove, supra n. 2, at 1088.

unregulated development and deployment of the technology; (2) the concern for the absence of law and policy that balance security and privacy; and (3) the fear of the abusive use of surveillance technology by police and private security personnel. Finally, commentators cite the recent exploitation of police video for profit as a reason for limiting the use of video surveillance and the videotaping of police activity. The survey of the technology is a reason for limiting the use of video surveillance and the videotaping of police activity.

16. See e.g. Burrows, supra n. 4, at 1109-1110 (citing Doe v. B.P.S. Guard Servs., Inc., 945 F.2d 1422, 1423 (8th Cir. 1991) (security guards filming fashion models undressing back stage at a convention center); People v. Dezek, 308 N.W.2d 652, 653 (Mich. App. 1981) (police video surveillance of restrooms at a rest stop); People v. Hunt, 259 N.W.2d 147, 148 (Mich. App. 1977) (police video surveillance of public restrooms); State v. Owczarzak, 766 P.2d 399, 400 (Or. App. 1988) (police installed cameras in public restrooms to catch males engaging in homosexual activities)). In 1972, Justice William O. Douglas dissented from the Supreme Court's decision not to grant a writ of certiorari in Williamson v. United States, 405 U.S. 1026, 1026 (1972), a case in which the federal appellate court approved the electronic interception of communications between a police informant and the suspected operator of a whiskey still. Justice Douglas observed that, although electronic eavesdropping had been justified as a necessary means of combating organized crime, government agencies, including the Army, actually used it to conduct surveillance of United States senators and representatives, the ACLU, the NAACP, the Urban League, college black studies programs, and antiwar groups. Id. at 1027-1028; see e.g. Chic. Laws. Comm. for Civil Rights Under L., Inc. v. City of Chic., 1985 WL 3450 (N.D. Ill. 1985) (classaction suit filed against Chicago police by various organizations involved in political, religious, educational, or social activities). In 2002 alone, segments on National Public Radio and dozens of articles in print media expressed concern for the development and rapid application of video monitoring technology. E.g. AP, Smile, You're on Surveillance Camera, Record C1 (Aug. 20, 2002); Adam Clymer, Surveillance Rules Are Needed To Save Privacy, Senators Say, N.Y. Times A18 (Aug. 2, 2002); Brian DeBose, Morella, Norton: Park Police Didn't Submit Camera Regulations, Wash. Times A12 (July 4, 2002); Benny Evangelista, Surveillance Society: Don't Look Now, But You May Find You're Being Watched, S.F. Chron. E1 (Sept. 9, 2002); Adam Goodheart, Public Cameras Accost Privacy, USA Today 11A (July 22, 2002); Bruce Landis, ACLU Seeks Policy on Video Surveillance, R.I. Providence J. Bull. B-05 (May 8, 2002); John Markoff, Protesting the Big Brother Lens, Little Brother Turns an Eye Blind, N.Y. Times C1 (Oct. 7, 2002); Dean E. Murphy, As Security Cameras Sprout, Someone's Always Watching, N.Y. Times 1-1 (Sept. 29, 2002); Melanie Scarborough, "Eyes...," Wash. Post A17 (June 4, 2002); William Walker, Coming Soon to a Video Camera Near You, Toronto Star B04 (May 12, 2002). Washington writer Adam Goodheart responds to the recent "ramping up" of video surveillance by suggesting that, "[before] Americans quietly accept such curtailments of privacy as a necessary cost of the war on terrorism, they should consider the threat this trend poses to our freedoms. They also should take a close look at evidence that suggests more surveillance cameras are unlikely to make our country more secure." Goodheart, supra, at 11A. Goodheart emphasizes the absence of warrant requirements, which characterize audio monitoring by law enforcement agencies, as a precondition to video monitoring. Id. Scarborough, supra, reports that crime has increased in London since 2001, despite the widespread use of video cameras. Clymer, supra, highlights the growing concern of the members of Congress, including Senators Charles E. Shumer of New York and John Edwards of North Carolina, that federal standards be established for video security technology.

17. See e.g. Burrows, supra n. 4, at 1109 (explaining that, "[i]f more American cities do turn to video surveillance, it probably will not take long before some entrepreneur . . . tries

2003] CCTV and Other Video Security Technology

It may be that the interest in video surveillance has persisted because of its growing use in the United Kingdom and elsewhere outside of the United States. At the time he wrote his article, Burrows reported more than 150,000 cameras, in more than seventy-five cities in England; these cameras were installed in response to rising street crime. 18 He also reported that many video clips were sold as "bootleg films" on the pornography market.¹⁹ Similar problems have occurred in France, where the police have broad powers over street video surveillance, and in Australia, Ireland, and Scotland.20 Also, the growing interest in video surveillance in the United States is certainly a consequence of the rapidly increasing use of the technology. As one commentator noted, "today there seem to be cameras everywhere." More than sixty metropolitan areas in the United States use video surveillance in public areas for law enforcement purposes—as a means of apprehending criminals after-the-fact and for crime prevention.²²

Cameras are also increasingly used in the workplace to monitor employee productivity, to deter theft, and to enhance workplace security.²³ In addition, cameras are now common in retail establishments to assist in loss prevention and customer safety.²⁴ Thus, surveillance cameras photograph a person who lives and works in a metropolitan area in the United States an average of twenty times per day.²⁵ Cameras are found at intersections, in apartment and office building lobbies, in parking lots, in stores, in

to use the footage from the cameras for a new television show."). Commentators argue that television shows featuring graphic video, like police chases or 911 rescues, may cause emotional or physical injury to suspects, victims, and their families. *E.g.* Burrows, *supra* n. 4, at 1108; *but see Vega-Rodriguez v. P.R. Tel. Co.*, 110 F.3d 174, 182 (1st Cir. 1997) (holding that fear that an employer will expand video surveillance into the restrooms, creating a "potential" privacy invasion, is not ripe for judicial review (emphasis in original)).

- 18. Burrows, supra n. 4, at 1099.
- 19. Id. at 1100.
- 20. Id. at 1101–1102. Burrows cites press accounts of the sale of videotapes of criminal activities and footage from hidden cameras on streets, in shopping malls, and in public toilets. Id. at 1099–1102 nn. 156–176.
- 21. Christopher S. Milligan, Facial Recognition Technology, Video Surveillance, and Privacy, 9 S. Cal. Interdisc. L.J. 295, 296 (1999).
 - 22. Id. at 301.
 - 23. Id. at 302.
 - 24. Id.

305

^{25.} Lawrence White, CLE Presentation, *Is the Right of Privacy Disappearing? Revisiting Issues of Privacy in the College and University Setting*, (Clearwater Beach, Fla., Feb. 12, 2000) (copy on file with Stetson University College of Law, Office for Continuing Legal Education).

banks, and in elevators.²⁶ Schools also utilize this technology for the safety and security of their community.²⁷ In short, both the number of cameras and the diversity of uses have multiplied exponentially since the technology was first introduced.

This history of video surveillance has reaffirmed the commonsense notion that all law-abiding citizens are vitally interested in efforts to reduce crime in the streets, in places of public accommodation, and in other vulnerable places (e.g., ATM machines). However, these same citizens worry about the unethical use (viewing, sale, etc.) of surveillance video by police and private security; its inherently indiscriminate and invasive character; and whether the cost of broad-scale video surveillance projects will be justified by meaningful increases in arrests and convictions, and significant decreases in criminal activity. It

As a result of these continuing interests and concerns, the legal and policy issues related to surveillance, in its broadest scope, remain to be further addressed by the courts, legislatures, and commentators. Throughout our discussion, we are mindful of Professor Daniel Solove's observation that surveillance is a different kind of privacy problem than the disclosure of private facts or information about a person.³² However, we fall short of making a clear choice between a traditional approach and a contextual ap-

^{26.} Id.

^{27.} Joan Gaustad, *The Fundamentals of School Security*, ERIC Digest No. 132 (1999–11–00) (available at http://www.ericfacility.net/ericdigests/ed436814.html).

^{28.} See e.g. Dunnigan v. Keane, 137 F.3d 117, 130 (2d Cir. 1998) (holding that a court may admit videotape from bank ATM to identify assailant).

^{29.} *Infra* n. 16 and accompanying text (discussing the abusive use of surveillance technology by police and private security personnel).

^{30.} See U.S. v. Torres, 751 F.2d 875, 883 (7th Cir. 1984) (permitting the use of "targeted" video surveillance only when the need for surveillance of criminal activity outweighs privacy concerns); accord U.S. v. Biasucci, 786 F.2d 504, 509 (2d Cir. 1986) (authorizing the use of video surveillance in "appropriate circumstances"). However, these cases involved surveillance of private premises, not public streets. Granholm, supra n. 3, at 691 n. 25.

^{31.} See Laura Linden, City of Oakland Will Not Use Street Surveillance Cameras, L.A. Daily J. 3 (Sept. 19, 1997) (noting a three-to-one vote of the Oakland City Council Public Safety Committee not to proceed with a plan for fifty video cameras to scan streets with zoom lenses). The ACLU, merchants, and local media described the plan as "Orwellian and a violation of the California Constitution's explicit right to privacy." *Id*.

^{32.} Solove, supra n. 2, at 1130. The intrusiveness of surveillance is direct because "Being watched can destroy a person's peace of mind, increase her self-consciousness and uneasiness to a debilitating degree, and can inhibit her daily activities," thus raising our interest in securing affirmative practices that restrict the power of the government or employers. Id.

2003] CCTV and Other Video Security Technology

proach to the issues raised by the use of CCTV and related technology.

III. CONSTITUTIONAL LAW AND PRIVACY PRINCIPLES GOVERNING THE USE OF VIDEO SECURITY TECHNOLOGY

A. Federal Law

The right of privacy is based on both constitutional and common-law grounds.³³ As a constitutional right, it is derived from the First, Third, Fourth, Fifth, Ninth, and Fourteenth Amendments, and from specific provisions of state constitutions.³⁴ In *Katz* v. *United States*,³⁵ the United States Supreme Court held that the government's electronic interception of the defendant's conversation in a phone booth violated his right of privacy if the defendant had an actual (subjective) expectation of privacy that society would recognize as reasonable.³⁶ *Katz* is the seminal case linking the concept of privacy to the Fourth Amendment and identifying its roots in the common law.³⁷ The subjective and ob-

307

^{33.} Electronic surveillance is not unconstitutional per se. *U.S. v. Martinez*, 498 F.2d 464, 467 (6th Cir. 1974), *cert. denied*, 419 U.S. 1056 (1974); *see also* 18 U.S.C. § 2510 (2000) (interception of communications); *State v. Diaz*, 706 A.2d 264, 265 (N.J. Super. App. Div. 1998) (holding that parents' arrangement with a private firm to install a videotape surveillance system in their home to record the conduct of a nanny hired to care for their children does not implicate federal or state constitutions (citing *U.S. v. Jacobsen*, 466 U.S. 109, 113 (1984))).

^{34.} See infra n. 85 and accompanying text (identifying states that have explicit constitutional protections of privacy); see e.g. Vega-Rodriguez, 110 F.3d at 183 (holding that, while employee surveillance by public employers raises Fourth Amendment concerns, Ninth Amendment and Fourteenth Amendment cases do not support a cause of action precluding video surveillance of work areas). The court held that Fourteenth Amendment privacy right cases generally protect an individual's autonomy in making significant personal decisions relating to things like marriage, contraception, and family relationships. Id.

^{35. 389} U.S. 347 (1967).

^{36.} *Id.* at 352. The Supreme Court refused to limit search and seizure protections to cases of physical intrusion, holding that the Fourth Amendment protects people, not places. *Id.* at 353. Canada recognized *Katz* in interpreting its search and seizure law, holding that, when a person has a reasonable expectation of privacy, the Charter of Rights and Freedoms prohibits the unrestricted, warrantless use of surveillance video. *Duarte v. Her Majesty The Queen*, [1990] 1 S.C.R. 30, 38.

^{37.} In Olmstead v. United States, 277 U.S. 438, 466 (1928), and later in Goldman v. United States, 316 U.S. 129, 134 (1942), the Supreme Court found similar surveillance permissible because it did not violate concepts of common-law trespass. Justice Louis D. Brandeis dissented in Olmstead, identifying a right of privacy in the common-law and describing it as "the right to be let alone." Olmstead, 277 U.S. at 478 (Brandeis, J., dissenting) (Justice Brandeis dissented on the basis of his seminal article with Samuel Warren, The Right of Privacy, 4 Harv. L. Rev. 193 (1890)); see also Kyllo v. U.S., 533 U.S. 27, 31

jective test established in *Katz* has continued to be the theoretical benchmark in video surveillance cases, ³⁸ and the Court has interpreted *Katz* to extend its protections to persons inside of their homes, where such technology intrudes upon expectations of privacy. ³⁹ Indeed, the Court's recent five-to-four decision in *Kyllo v. United States*, ⁴⁰ specifically limiting police use of a thermalimaging device aimed at a private home, suggests that the warrantless use of video cameras might be suspect when the technology allows intrusion beyond the naked eye into areas where expectations of privacy are heightened.

At the outset of its opinion in *Kyllo*, the majority noted that the warrantless search of a private home is generally unconstitutional. Therefore, the issue in the majority of cases is determining when visual surveillance becomes a "search" within Fourth Amendment principles. Early historical precedent permitted ordinary visual observation from outside the home because it was nontrespassory, and modern cases reason, *a fortiori*, that law enforcement officers are not required to ignore ordinary visual observations of a private home from a public street. The rationale of the modern cases is not that such activity is a "reasonable search," but that it is not a "search" at all. The *Kyllo* majority suggests that the key factor in determining whether visual surveillance constitutes a search is the violation of a subjective expectation of privacy that society recognizes as reasonable—the so-called *Katz* benchmark.

Applying the *Katz* test, the Court in *Kyllo* held that the warrantless use of thermal imaging technology by a law enforcement officer on a public street is subject to Fourth Amendment restric-

^{(2001) (}citing *Olmstead* to explain that Fourth Amendment jurisprudence has roots in common-law trespass); Solove, *supra* n. 2, at 1100–1101 (discussing the Brandeis and Warren article).

^{38.} See Granholm, supra n. 3, at 692 n. 26 (citing People v. Smith, 360 N.W.2d 841, 853 (Mich. 1984), to explain that courts will determine the defendant's reasonable expectation of privacy by looking at the "totality of the circumstances").

^{39.} See e.g. Kyllo, 533 U.S. at 40 (finding that the government's use of a thermalimaging device on the defendant's house constituted an unlawful search).

^{40. 533} U.S. 27.

^{41.} Id. at 31 (citing Ill. v. Rodriguez, 497 U.S. 177, 181 (1990), and Payton v. N.Y., 445 U.S. 573, 586 (1980)).

^{42.} E.g. id. at 32 (citing Cal. v. Ciraolo, 476 U.S. 207, 213 (1986)).

^{43.} E.g. id. (citing Dow Chem. Co. v. U.S., 476 U.S. 227, 234-235, 239 (1986)).

^{44.} Id. at 33.

tion when it enhances that officer's ordinary perception to the extent of allowing the officer to detect "information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area." The Court's clear concern was intrusion, by sense-enhancing technology, into the interior of a home because it is there that basic notions of privacy take notice of subjective—and reasonable—expectations of privacy.

The Court held that the use of thermal-imaging technology to detect heat being generated from high-intensity lamps used to grow marijuana inside a home was a "search" because no ordinary observation from outside the home could have detected the relative heat that allowed the inference of illegal activity. ⁴⁷ The Court reached this conclusion even though the technology employed detected only heat radiating from the outside of the house being scanned—making clear its intent to fashion a rule of law to properly account for more sophisticated forms of surveillance technology in use, or being developed, for law-enforcement applications. ⁴⁸

The government's arguments in *Kyllo*, accepted in part by the dissent, asserted that a fundamental difference exists between "off-the-wall" observations and "through-the-wall" surveillance of a house. ⁴⁹ The majority rejected such a bright distinction, relying on *Katz*, in which the eavesdropping device employed detected only sound waves reaching the exterior of a phone booth. ⁵⁰ It also rejected the government's argument that the warrantless use of imaging technology was appropriate because it did not "detect private activities occurring in private areas." ⁵¹ That argument, the

^{45.} Id. at 34 (quoting Silverman v. U.S., 365 U.S. 505, 512 (1961)).

^{46.} There is judicial opinion, predating *Kyllo*, suggesting that judicial concern for the warrantless use of video monitoring extends beyond the home. In her dissenting opinion in *Cowles v. State*, 23 P.3d 1168, 1176–1177 (Alaska 2000), Alaska Supreme Court Justice Dana Fabe observed that Alaska's constitutional privacy provisions may have been enacted to protect against extensive governmental use of electronic surveillance techniques, including video technology. Citing precedent from Alaska, Montana, and Hawaii, Justice Fabe suggested that judicial prohibition of warrantless audio monitoring illustrated the concern for "The corrosive impact of warrantless . . . monitoring on our sense of security" *Id.* at 1177 (quoting *State v. Glass*, 583 P.2d 872, 877 (Alaska 1978), as suggesting constitutional limitations on both audio and video monitoring).

^{47.} Kyllo, 533 U.S. at 34-35.

^{48.} Id. at 35-36.

^{49.} Id. at 35.

^{50.} Id.

^{51.} *Id*. at 37.

310

Court observed, was based on the Court's earlier decision in *Dow Chemical Co. v. United States*,⁵² approving advanced video photography of the defendant's industrial site by EPA agents—a situation that does not raise the Fourth Amendment's protection of a person's home.⁵³ In sum, the majority rejected any bright-line rule based on the relative sophistication of emerging technology, in favor of a rule that reaffirms the Constitution's concern for the inherently private nature of the home.⁵⁴

The Supreme Court's decision in *Kyllo* established general limitations on the warrantless use of imaging technology—beyond mere thermal-imaging devices—in "home" cases, suggesting that the nonpublic use of any imaging device to explore the details of a home, which exploration would not otherwise be obtainable without some type of physical intrusion, is a "search" that is subject to constitutional restraints. However, post-*Katz* cases have substantially weakened the expectation of privacy outside of the home.⁵⁵

^{52. 476} U.S. 227.

^{53.} Kyllo, 533 U.S. at 37. The majority observed that, in the home, "all details are intimate details" because of the constitutional concern for the sanctity of the home, as compared with other places where there might be some expectation of privacy. Id. (emphasis in original); cf. U.S. v. Heath, 259 F.3d 522, 531 (6th Cir. 2001) (holding that the defendant had a protected privacy interest in the common area of his apartment building, where police gained access using keys given to them by another suspect); State v. Reinier, 628 N.W.2d 460, 467 (Iowa 2001) (holding that police intrusion, without a warrant, onto a suspected drug dealer's porch violates Fourth Amendment protections because the owner has a privacy interest in the porch portion of his premises); State v. Stott, 794 A.2d 120 (N.J. 2002) (holding that a person committed to a state mental hospital has a constitutionally protected privacy interest, under the federal constitution, against a warrantless search of his or her assigned room by police); State v. Vrieling, 28 P.3d 762, 766 (Wash. 2001) (holding that state constitutional privacy provisions do not extend to the occupant of a motor home the same protections of privacy associated with a customary home).

^{54.} Kyllo, 533 U.S. at 37–38. The dissent criticized the majority's general perception of the need for a rule that anticipates developing technology and its non-recognition of the principle that a person is not entitled to Fourth Amendment protections for activities knowingly exposed to the public, even in his or her own home. Id. at 42–44 (Stevens, J., dissenting). The dissent would have the law step in if the sense-enhancing technology deployed would allow law enforcement agents to detect the content of conversation or activity inside a home, phone booth, etc., which would otherwise be available only to someone inside the private area. Id. at 57.

^{55.} Burrows, supra n. 4, at 1088 (citing Dow Chem. Co., 476 U.S. at 239 (aerial photography, by EPA, of company's complex); Tex. v. Brown, 460 U.S. 730 (1983) (police officer's use of a flashlight to illuminate the inside of a motorist's car during routine driver's license checkpoint); Fla. v. Riley, 488 U.S. 445, 447–448 (1989) (aerial surveillance of a greenhouse); Ciraolo, 476 U.S. at 209 (aerial photographs of marijuana growing in the defendant's backyard). In Ciraolo, a five-to-four majority of the Supreme Court held that, although the defendant erected a ten-foot fence around his backyard with the intent to obstruct the view of his marijuana growing activity, officers who observed his plants while

Indeed, Burrows and Granholm conclude that the Fourth Amendment is generally not supportive of a constitutional challenge to silent video surveillance of public streets, sidewalks, and parks because persons do not have a reasonable expectation that they will be free from observation in such public settings.⁵⁶

Granholm argues, however, that a citizen might have a reasonable expectation that technology used to observe her in public places should not be so intrusive as to focus upon the letter she is reading or the movement of her lips; nor should such technology record her as she walks with a secret lover. The Granholm's argument is based upon her reading of the "plain-view" doctrine in search and seizure cases. The argues that, although courts have held that a view open to outsiders mitigates the suspect's reasonable expectation of privacy, reliance on the plain-view doctrine is misplaced if video surveillance includes enhancement features such as telescopic lenses or film-recording devices. The solution of privacy is such as telescopic lenses or film-recording devices.

Granholm insists that the plain-view doctrine is based upon the premise that the discovery of the evidence in question is inadvertent. ⁶⁰ She reasons that, when an enhanced video device is deployed to observe activity, the observation "is intrinsically advert-

flying in a private plane at an altitude of 1,000 feet did not violate the defendant's reasonable expectations of privacy. 476 U.S. at 213–214. The Court held that the Fourth Amendment protection of the home was never meant to preclude observations that may be made by law enforcement officers from public thoroughfares. Id. Thus, a homeowner's steps to restrict some views do not "preclude an officer's observations from a public vantage point where he has a right to be and which renders the [defendant's] activities clearly visible." Id. at 213. Therefore, the defendant's subjective expectation of privacy was not objectively reasonable. Id. at 214.

- 56. Burrows, *supra* n. 4, at 1090; Granholm, *supra* n. 3, at 694–695.
- 57. Granholm, *supra* n. 3, at 695. Granholm argues that this limitation of video and audio surveillance is the essence of a reasonable application of the Supreme Court's decision in *Katz. Id.*
- 58. See id. at 696 (citing Coolidge v. N.H., 403 U.S. 443 (1971)). The Coolidge Court limited the doctrine to situations in which police seize an object pursuant to a prior, valid search (i.e., pursuant to a warrant), or "a judicially recognized exception to the warrant requirement." Id. at 696 n. 43.
- 59. *Id.* at 697. Granholm's distinction has merit. In *Vega-Rodriguez*, the court observed that arguments justifying street video surveillance emphasize the constitutional parity between observations made with the naked eye (by an officer who could be assigned to the streets) and observations recorded by an openly displayed video camera having no greater range than the officer's naked eye. 110 F.3d at 181. Scarborough suggests that a significant reason for the concern about video monitoring is that emerging technology allows 360-degree views and magnification exceeding seventeen times the capability of the naked eye. Scarborough, *supra* n. 16, at A17.
 - 60. Granholm, supra n. 3, at 697.

ent, adverse, and intrusive."⁶¹ This characterization of enhanced video monitoring focuses legal inquiry on the most fundamental purpose of federal and state privacy protections: "[T]o safeguard the privacy and security of individuals against arbitrary invasions by government officials."⁶² However, this aspect of Granholm's argument predates Supreme Court decisions approving aerial searches in drug cultivation cases and other recent cases, which extend the constitutional debate about video security technology to settings far beyond the public street, park bench, or sidewalk.

L.R. Willson & Sons, Inc. v. Occupational Safety & Health Review Commission considered both the issue of expectation of privacy and Granholm's concern for "enhancements" such as zoom lenses. In L.R. Willson, the Secretary of Labor cited the defendant company for violations of the Occupational Safety and Health Act of 1970 (OSHA) after discovering that employees were working on structural steel more than eighty feet above the ground without the benefit of mandated "fall protective devices." An OSHA compliance officer, standing at the window of a hotel room across the street from the worksite and using a "16" power camera lens, observed the employees and documented the violation. Upholding an administrative law judge's admission of the videotape at an evidentiary hearing, the appellate court found that, "[a]lthough surveillance is a type of search that can invoke

^{61.} *Id.* Granholm explains that, "[i]f a video camera can zoom in to focus on facial expressions, a license plate, or a letter we may be carrying," the camera's capability exceeds the senses of the police on the beat and any argument that the camera is simply an extension of the police is a flawed argument. *Id.* at 698. Granholm cites *People v. Fly*, 110 Cal. Rptr. 158, 159–160 (Cal. App. 2d Dist. 1973), wherein the court held that an officer's observation of marijuana growing in the defendant's enclosed yard through a telescope was a search because the officer had "wedged" himself between two buildings and thus, had assumed an unusual vantage point. *Accord U.S. v. Cuevas-Sanchez*, 821 F.2d 248, 251 (5th Cir. 1987) (holding that police video surveillance of defendant's backyard qualified as a search).

^{62.} $State\ v.\ Bonnell,\ 856\ P.2d\ 1265,\ 1272\ (Haw.\ 1993)\ (quoting\ Camara\ v.\ Mun.\ Ct.,\ 387\ U.S.\ 523,\ 528\ (1967)).$

^{63. 134} F.3d 1235 (4th Cir. 1998).

^{64.} Id. at 1238-1239.

^{65. 29} U.S.C. §§ 651–678 (2000).

^{66. 134} F.3d at 1237 (these devices were required by 29 C.F.R. § 1926.750(b)(1)(ii)).

^{67.} *Id.* The discovery was initially made by an Assistant Secretary of Labor for Occupational Safety and Health, from his room at the hotel. *Id.* After observing the workers, the Assistant Secretary telephoned the local OSHA compliance officer, who received permission from the hotel to videotape the worksite from the window of the Assistant Secretary's room. *Id.* The compliance officer then visited the worksite, presented his credentials, and interviewed the employees. *Id.*

313

Fourth Amendment protections if performed unreasonably, [the compliance officer's enhanced] observations were not unreasonable." The court held that, since the video disclosed only what was easily observable by anyone on one of the hotel's upper floors, the employer had no reasonable expectation of privacy. Quoting Secretary of Labor v. Concrete Construction Co., the court explained that "there is no constitutional violation when an inspector makes observations from areas on commercial premises that are out of doors and not closed off to the public."

Granholm's second argument is that mass citizen surveillance should be unconstitutional because, like drug testing and sobriety checkpoints, it lacks the precondition of reasonable suspicion, thereby rendering people "guilty until proven innocent." It also lacks the justification for mass searches at airports and government buildings. Granholm argues that cases allowing mass searches at airports and government buildings are based upon the presence of proven, present risks of violence in these settings, which are not present in general surveillance scenarios. She concludes that the undifferentiated threat presented by

^{68.} Id. at 1238.

^{69.} Id.

^{70. 15} O.S.H.C. 1614 (O.S.H.A. 1992).

^{71.} *L.R. Willson*, 134 F.3d at 1238. The court noted the use of a high-powered lens in shooting the videotape, but found that the employer left the worksite "open to observation from vantages outside its control." *Id.* Thus, the court concluded that a sustained view from a hotel across the street from the construction site was not an unreasonable intrusion into the employer's "private space." *Id.* The court also held that the use of the video camera did not violate Section 8(a) of the Act requiring that an inspector present his credentials before "inspecting" a site, or the employer's "walkaround rights" under Section 8(e) of the Act. *Id.* at 1239–1240.

^{72.} Granholm, *supra* n. 3, at 700. For a case regarding the constitutionality of government checkpoints set up to detect drunk drivers, see *Michigan Department of State Police v. Sitz*, 496 U.S. 444 (1990).

^{73.} Granholm, *supra* n. 3, at 703–704. At its root, Granholm's argument raises an interpretation of state and federal privacy protections that extend to an individual, wherever he or she would reasonably expect freedom from governmental intrusion. *See e.g. Bonnell*, 856 P.2d at 1275 (explaining that privacy goes wherever the person goes).

^{74.} Granholm, supra n. 3, at 703–704 (citing 14 C.F.R. § 121.538 (1987) (requiring air carriers to use screening devices designed to deter passengers from carrying explosives or weapons aboard an aircraft); Downing v. Kunzig, 454 F.2d 1230, 1231 (6th Cir. 1972); U.S. v. Lopez, 328 F. Supp. 1077, 1082 (E.D.N.Y. 1971); U.S. v. Bell, 335 F. Supp. 797, 799 (S.D.N.Y. 1971), affd, 464 F.2d 667 (2d Cir. 1972)).

^{75.} Granholm, *supra* n. 3, at 702–705 (citing *Collier v. Miller*, 414 F. Supp. 1357, 1367 (S.D. Tex. 1976) (determining that searching university sports-arena patrons did not fall under the courthouse or airport exceptions to a warrant requirement); *Jacobsen v. Seattle*, 658 P.2d 653, 656 (Wash. 1983) (holding that the danger posed by patrons at a rock concert

general crime statistics does not justify the use of highly enhanced surveillance technology. Indeed, she explains that the actual settings in which video surveillance is frequently used are not inner-city, high crime areas where the safety of poor people is threatened, but areas like shopping malls and upscale entertainment districts instead (e.g., Bricktown, Detroit), where the intent is to protect suburban shoppers and the economic well-being of store and club owners.

Burrows suggests that attempts to prevent the reasonable use of video surveillance of public places—on the ground that such surveillance violates federal privacy concepts—are also likely to be unsuccessful. Although he reminds us of the importance of the Supreme Court's decision in *Griswold v. Connecticut* and its progeny, he suggests that members of the current Court have rejected the right of privacy in public places when balanced against the state's interest in deterring criminal activity. The

is far less than that posed by the threat of terrorist bombings of courtrooms and attempts to hijack airplanes)). Granholm acknowledges cases to the contrary. Granholm, supra n. 3, at 705 n. 80 (citing Jensen v. City of Pontiac, 317 N.W.2d 619, 624 (Mich. App. 1982) (holding that the search of patrons entering a stadium is justified by threat of harm caused by unknown assailants throwing container-type objects)); see also Norwood v. Bain, 143 F.3d 843, 850 (4th Cir. 1998) (approving videotaping of license checks of motorcycle riders seeking to enter fairgrounds for a motorcycle rally, based upon reliable reports of potential violence involving rival clubs). The court in Wheaton v. Hagan explains the distinction. 435 F. Supp. 1134, 1145-1146 (M.D.N.C. 1977). Citing United States v. Edwards, 498 F.2d 496 (2d Cir. 1974), and United States v. Moreno, 475 F.2d 44 (5th Cir. 1973), in addition to the cases cited by Granholm, the Wheaton court observed that the factors advanced in the airport and courthouse search cases are the public necessity for warrantless searches, the efficacy of the search, and the nature of the intrusion involved. Wheaton, 435 F. Supp. at 1145. In the seminal cases, the documentation of bombings and other acts of violence in the late 1960s and early 1970s satisfied the public safety factor. Id. In contrast, the court explained, as unruly as patrons of arenas and coliseums might be, the dangers posed by these actors are substantially less than the dangers which generally justify suspending the warrant requirement in courthouse and airport cases. Id. The court was also concerned that, in the arena cases, searches tended to be random, singling out certain individuals, thereby exposing them to a stigma or embarrassment. Id. at 1146. The court held that, unless alternatives to random searches are adopted, a search of an arena patron should comply with the standard announced in Terry v. Ohio, 392 U.S. 1, 21 (1968). Wheaton, 435 F. Supp. at 1146. Under Terry, "The [searching] officer must be able to point to specific and articulable facts which . . . together with rational inferences . . . [would] reasonably warrant that intrusion." 392 U.S. at 21.

- 76. Granholm, supra n. 3, at 706.
- 77. Id.
- 78. Burrows, supra n. 4, at 1091.
- 79. 381 U.S. 479 (1965).
- 80. Burrows, supra n. 4, at 1091 (citing William H. Rehnquist, Is an Expanded Right of Privacy Consistent with Fair and Effective Law Enforcement? Or: Privacy, You've Come

315

2003]

limited precedent dealing with the expectation of privacy is in that context, i.e., the video surveillance of suspected criminal activity. 81

In these cases, federal courts have found some expectation of privacy on business premises or within buildings, but have upheld video surveillance orders.⁸² These cases deal with the intrusive nature of video surveillance in situations where there is some legitimate expectation of privacy and where, therefore, the need for surveillance must be justified. Such surveillance intrusions are also the concern of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended.⁸³ Unfortunately, the federal

a Long Way, Baby, 23 U. Kan. L. Rev. 1, 5 (1974)); see also id. at 1094 (discussing Laird v. Tatum, 408 U.S. 1, 10 (1972), which affirmed the refusal of an injunction preventing army officials from engaging in covert surveillance of civilian political activities where meetings were public).

81. See infra n. 82 and accompanying text (citing cases involving video surveillance of suspected criminal activity).

82. E.g. U.S. v. Wilson, 116 F.3d 1066, 1074 (5th Cir. 1997) (permitting video surveillance of undercover drug purchases from gang members); U.S. v. Mesa-Rincon, 911 F.2d 1433, 1445 (10th Cir. 1990) (authorizing Secret Service installation of a television camera to film defendants' counterfeiting operation); cf. U.S. v. Pui Kan Lam, 483 F.2d 1202, 1206 (2d Cir. 1973), cert. denied, 415 U.S. 984 (1974) (reasoning that defendants had no justifiable expectation of privacy while in the house of complete strangers when they had gained entry by false representations).

83. Burrows, supra n. 4, at 1096-1097 (discussing Congress and video surveillance); 18 U.S.C., §§ 2510-2521 (1994), as amended by the Electronic Communication Privacy Act of 1986, Pub. L. 99-508, Pub. L. 103-414, and Pub. L. 105-153 (1997); see U.S. v. Bailey, 607 F.2d 237, 240-241 (9th Cir. 1979) (holding that Title III is constitutional under the Fourth Amendment (citing U.S. v. Turner, 528 F.2d 143, 158-159 (9th Cir. 1975), cert. denied sub nom. Hackett v. U.S., 429 U.S. 837 (1976))). The Act requires application for a court order to intercept communications in connection with the investigation of enumerated crimes, but does not specifically subsume the use of silent video surveillance. See Cuevas-Sanchez, 821 F.2d at 251 (noting that Title III does not specifically include video surveillance); Ricks v. State, 537 A.2d 612, 613 (Md. 1988) (discussing the Act's requirements). The purpose of the Act is to protect individual privacy while permitting limited governmental surveillance, in accordance with uniform standards, when necessary for effective law enforcement. Dowd v. Calabrese, 101 F.R.D. 427, 435 n. 22 (D.D.C. 1984); Application of U.S. Authorizing Interception of Wire Commun., 413 F. Supp. 1321, 1331 (E.D. Pa. 1976). For an excellent discussion of Title III, see Karen A. Springer, In God We Trust: All Others Who Enter This Store are Subject to Surveillance, 48 Fed. Commun. L.J. 187 (1995). It is noteworthy that, while Section Eight of Canada's Charter of Rights and Freedoms (protecting against unreasonable search and seizure) is similarly silent as to video surveillance, the Supreme Court of Canada has interpreted Section Eight to cover both audio and video surveillance. See Wong v. Her Majesty The Queen, [1990] 3 S.C.R. 36, 44 (citing Duarte, 1 S.C.R. at 34, and observing that,

[i]n Duarte, this Court held that unauthorized electronic audio surveillance violates s. 8 of the Charter. It would be wrong to limit the implications of that decision to that particular technology. Rather what the court said in Duarte must be held to embrace all existing means by which the agencies of the state can electronically intrude

courts appear to be divided on the application of the Act's requirements to targeted silent video surveillance, where justifiable expectations of privacy might exist. Thus, federal law in this area remains less than fully conclusive.

B. State Court Cases and State Privacy Law

The states have fashioned concepts of privacy in constitutional provisions and judicial pronouncements. A number of states, including Alaska, California, Florida, Hawaii, Illinois, Michigan, Montana, New Hampshire, Oregon, Pennsylvania, and

on the privacy of the individual, and any means which technology places at the disposal of law enforcement authorities in the future." (emphasis added)).

The Wong Court cited Justice Brandeis' "prophetic dissent" in Olmstead, 277 U.S. at 474, wherein Brandeis "foresaw that the progress of science in furnishing government with the means of 'espionage' could not be expected to stop with wiretapping." Wong, 3 S.C.R. at 44.

84. Compare e.g. Biasucci, 768 F.2d at 510 (applying Title III to video surveillance "as a measure of the government's constitutional obligation"); Cuevas-Sanchez, 821 F.2d at 251 (applying Title III to the government's video surveillance of defendant's backyard); Torres, 751 F.2d at 880–884 (applying Title III to the F.B.I.'s video surveillance of apartments used by terrorists to manufacture bombs); Mesa-Rincon, 911 F.2d at 1445 (applying Title III to video surveillance) with U.S. v. Foster, 985 F.2d 466, 469 (9th Cir. 1993) (holding that videotaping the defendant did not violate the Electronic Privacy Act where a number of persons were present and the taping occurred with the consent of the owner of the premises); U.S. v. Taketa, 923 F.2d 665, 674 (9th Cir. 1991) (holding that silent video taping does not come within the provisions of Title III); In re Order Authorizing Interception of Oral Commun. & Video Surveillance, 513 F. Supp. 421, 423 (D. Mass. 1980) (holding that Title III is not applicable to silent video surveillance). Diaz emphasizes the Seventh Circuit's comment in Torres that,

it is anomalous to have detailed statutory regulation of bugging and wiretapping but not of television surveillance, in Title III, and detailed statutory regulation of television surveillance of foreign agents but not of domestic criminal suspects, in the Foreign Intelligence Surveillance Act. . . . But judges are not authorized to amend statutes even to bring them up to date.

Diaz, 706 A.2d at 267-268 (quoting Torres, 751 F.2d at 855-856); cf. U.S. v. Andonian, 735 F. Supp. 1469, 1472 (C.D. Cal. 1990) (reasoning that legislative history of 1986 amendments to Title III suggests that the statute would apply to the audio portion of a surveillance but not the video portion), aff'd, 29 F.3d 634 (9th Cir. 1994). For a discussion of the use of a "highlighted portion" of a videotape in criminal proceedings, see United States v. Hardwell, 80 F.3d 1471, 1492-1493 (10th Cir. 1996). Canada appears to follow Biasucci and holds that video surveillance of a hotel room would normally constitute a "search," thereby requiring a warrant. Wong, 3 S.C.R. at 54 (citing Stoner v. Cal., 376 U.S. 483, 490 (1964), regarding a person's reasonable expectation of privacy when occupying a hotel room). A majority of the Court in Wong held that tapes from the search in question, although including video surveillance not authorized by a court, did not "bring the administration of justice into disrepute" because the police acted in good faith with what they believed was the law. Wong, 3 S.C.R. at 59. The Court held, however, that unauthorized, surreptitious electronic surveillance violates Section Eight of the Charter of Rights and Freedoms when the target of the surveillance has a reasonable expectation of privacy. Id. at 53.

2003] CCTV and Other Video Security Technology

Texas, have explicit constitutional protections of privacy, some of which limit search and seizure, including wire and electronic communications surveillance, which Supreme Court precedent might permit. However, several states have permitted video surveillance when supported by a legitimate public interest in newsworthy information. Indeed, the public interest in crime can overcome personal concerns for privacy even in situations in which the publication of videotaped accounts causes emotional upset. The series of the publication of videotaped accounts causes emotional upset.

State law, adopting the Katz standard, may permit targeted video surveillance. In Ricks v. State, 88 the Baltimore, Maryland, police department employed surreptitious, nonconsensual video surveillance, pursuant to a court order, as part of an extensive narcotics investigation of premises allegedly being used by the defendants as a "processing house" or "cut house," where the defendants diluted and packaged controlled, dangerous substances for street sale.89 Following the defendants' arrest, based upon a search warrant, the Maryland Court of Special Appeals upheld the court-ordered surveillance under Maryland's Wiretap and Electronic Surveillance Act. 90 The court noted the defendants' admission that the federal Omnibus Crime Control and Safe Streets Act of 1968, after which the Maryland wiretap statute was modeled, did not regulate video surveillance and that the Maryland statute did not expressly contemplate video surveillance. 91 The court held, therefore, that the Maryland Wiretap and

317

^{85.} Burrows, supra n. 4, at 1113-1114.

^{86.} *Id.* at 1114–1115 (citing *Gill v. Hearst Publg. Co.*, 239 P.2d 636 (Cal. 1952), and *DeGregorio v. CBS*, 473 N.Y.S.2d 922 (Sup. Ct. 1984)).

^{87.} Burrows, *supra* n. 4, at 1116–1119 (citing *Cape Publications, Inc. v. Bridges*, 423 So. 2d 426, 427 (Fla. 1982) (newspaper publication of a photograph taken of a rape victim at the scene of the crime was held newsworthy); *Waters v. Fleetwood*, 91 S.E.2d 344, 348 (Ga. 1956) (newspaper publication of photographs of a murdered fourteen-year-old girl was held newsworthy)).

^{88. 520} A.2d 1136 (Md. Spec. App. 1987), aff'd, 537 A.2d 612 (Md. 1988).

^{89.} *Id.* at 1138. The lower court allowed police to install a small video camera in the ceiling of the apartment to record the illegal activities. *Id.* The court also authorized the use of electronic listening and recording devices. *Id.*

^{90.} *Id.* at 1139, 1142. The defendants argued that the surveillance violated both the Maryland Wiretap and Electronic Surveillance Act and the Fourth Amendment to the United States Constitution. *Id.* at 1138.

^{91.} *Id*. at 1139.

Electronic Surveillance Act did not proscribe or regulate silent video surveillance of suspected criminal activity. 92

As to the defendants' Fourth Amendment argument, the court reasoned that the proponent of a motion to suppress has the burden of proving that the video surveillance in question violates a legitimate expectation of privacy in the invaded place. The Maryland Court of Appeals, citing *Smith v. Maryland*, held that the defendant must demonstrate, by his conduct, that he "has exhibited a subjective expectation of privacy"—that he seeks to preserve something as private—and that his expectation "is one that society is prepared to recognize as reasonable"—that is, whether the defendant's expectation, viewed objectively, is justifiable under the circumstances. Some states have constitutional provi-

^{92.} Id. (citing Biasucci, 786 F.2d at 809 (permitting video surveillance of the "business" offices of a loan-sharking operation); Torres, 751 F.2d at 877 (permitting video surveillance of terrorist "safe houses," used to assemble bombs, on a showing that audio devices alone might be neutralized if the defendants played music, used code, or assembled bombs in silence); In re Order Authorizing Interception of Oral Commun. & Video Surveillance, 513 F. Supp. at 422–423 (allowing video surveillance within a dwelling when alternative investigative procedures unlikely to identify participants in criminal activities); People v. Teicher, 422 N.E.2d 506, 513 (N.Y. 1981) (permitting installation of a camera in the office of a dentist suspected of sexually assaulting female patients)); see Ruth Hochberger, Appellate Division Approves Video Surveillance by Police, 37 N.Y. L.J. 1, 1 (Feb. 25, 1980) (discussing Teicher, 422 N.E.2d 506), which affirmed defendant's conviction based on evidence of sexual abuse obtained via video surveillance of defendant's office).

^{93.} Ricks, 520 A.2d at 1140 (citing Rakas v. Ill., 439 U.S. 128, 131 (1978)).

^{94. 442} U.S. 735, 740 (1979).

^{95.} Ricks, 537 A.2d at 619. Finding that the defendants may have had a reasonable expectation of privacy under the facts of the case, the Maryland Court of Appeals held that the video surveillance was conducted in accordance with Fourth Amendment requirements and consistent with the required showings under Title III of the Omnibus Crime Control and Safe Streets Act (OCCSSA). Id. at 613, 620-621. The Ricks standard is explained in McCray v. State, 581 A.2d 45 (Md. Spec. App. 1990). In McCray, the defendant was suspected of procuring false driver's licenses for persons whose licenses had been suspended or revoked. Id. at 46. Police conducted a warrantless video surveillance of the defendant, videotaping him crossing the street to a state motor vehicle administration office. Id. at 47. The court held that such surveillance did not implicate the privacy concerns in Ricks because the videotaping of the defendant took place only when he was crossing the street and entering the Motor Vehicle Administration (MVA) office in full public view. Id. at 48. The court held that a person does not have a reasonable expectation of privacy when he or she is walking along public sidewalks, streets, or parking lots, or in similar locations in full public view. Id. (citing Gary C. Robb, Police Use of CCTV Surveillance: Constitutional Implications and Proposed Regulations, 13 U. Mich. J. L. Ref. 571 (1980)); see also Diaz, 706 A.2d at 266-267 (finding that New Jersey's Wiretap Act, modeled after Title III of the OCCSSA, does not subsume silent video surveillance, and the legislative history of the federal legislation indicates that the exclusion was deliberate). However, the warrant provisions of the New Jersey statute govern the admissibility of a videotape with sound recording in a criminal proceeding. *Id*.

sions that prohibit police use of video street surveillance cameras with zoom lens capability, or other intrusive surveillance. Burrows cites, as an example, the decision in *Hawaii v. Bonnell*, the held that police video surveillance of an employee break room, without a warrant, to investigate alleged gambling activities violated the Hawaii Constitution. He also cites Montana's compelling governmental interest requirement to justify excessively intrusive surveillance. However, when video-assisted street surveillance is limited in its intrusiveness, its use in reducing traffic violations or crime may be justified and upheld.

In recent years, video surveillance technology has been the subject of legislative efforts in a number of states. ¹⁰¹ These legislative initiatives capture the full spectrum of the debate over the value and concern implicated by the technology's use. In California, for example, the legislature enacted a bill, vetoed by the governor, that would have prohibited a school board from installing a video surveillance camera in any public place on a school site, unless the board first adopted a policy stating the purpose and the need for the surveillance. ¹⁰² New Jersey proposed legislation that would criminalize surreptitious use of video surveillance in

^{96.} See Linden, supra n. 31, at 3 (citing the concern of Oakland city officials that such surveillance would violate the California Constitution).

^{97. 856} P.2d 1265

^{98.} Burrows, *supra* n. 4, at 1119 n. 321. The *Bonnell* Court noted that fifty video tapes with 1,200 hours of footage, obtained from a hidden video camera in an employee break room, disclosed only a few minutes of conduct which might reflect misdemeanor-level gambling activity. 856 P.2d at 1271. More importantly, the Court held that the Hawaii Constitution protects legitimate expectations of privacy wherever an individual may go. *Id.* at 1275. Thus, even in a public park, an individual may have an expectation of privacy that should not be invaded by warrantless video surveillance absent exigent circumstances. *Id.* at 1278

^{99.} Burrows, *supra* n. 4, at 1121; *see State v. Brown*, 755 P.2d 1364, 1369 (Mont. 1988) (approving consensual warrantless monitoring of face-to-face conversation, but observing that privacy might preclude such interception when none of the participants have consented to the surveillance).

^{100.} Security Industry Association, Second Annual Report on CCTV for Public Safety, app. 8, 153 [hereinafter SIA Report] (discussing proposed legislation in Maryland for the use of video cameras to capture images of automobiles and license plates entering intersections after traffic signals have turned red); SIA Report, supra, at app. 12, 211 (discussing legislation in Illinois to enhance video surveillance technology by informing merchants to install a measurement device within the picture to better show the criminal's height and circ.)

^{101.} *Infra* nn. 102–106 and accompanying text (discussing legislative initiatives in California, New Jersey, New York, and Rhode Island).

^{102.} Cal. Assembly 614, 1999–2000 Reg. Sess. (Sept. 9, 1999) (vetoed Oct. 19, 1999).

any private place. 103 In New York, bills have been introduced that would (1) prohibit video surveillance in certain rooms, including fitting rooms, restrooms, toilets, bathrooms, washrooms, or showers on premises used for commercial purposes or which provide services to members of the public, or in rooms assigned to guests in a hotel;¹⁰⁴ and (2) provide for the creation of the crime of surreptitious video surveillance in a private dwelling without consent. 105 Finally, Rhode Island enacted legislation that provides for new audio-video surveillance cameras for the next five years to

^{103.} N.J. Sen. 300, 209th Leg., 2000 Sess. (Dec. 29, 1999).

^{104.} N.Y. Assembly 2979, 22d Leg. Sess., 1999-2000 Reg. Sess. (Jan. 27, 1999). The Florida Legislators were concerned about inappropriate, private use of silent video, which led to a statute prohibiting a person from secretly observing, photographing, or videotaping another person with lewd or indecent intent when the victim is in a dwelling, structure, or conveyance that provides a reasonable expectation of privacy. Fla. Stat. § 810.14

Emerging cases suggest that the language of statutes establishing criminal penalties may be strictly construed. See State v. Glas, 54 P.3d 147 (Wash. 2002) (holding that defendants' use of still photography or video cameras to photograph under the skirts of female victims in public places did not violate Washington's voyeurism statute). The Court repeatedly noted that the statute's clear language made it a crime to engage in so-called "upskirt" photographing or filming "while the person [being viewed, photographed, or filmed] .. is in a place where he or she would have a reasonable expectation of privacy." Id. at 150 (emphasis in original). The victims photographed in public areas of a mall, or in public areas of the Seattle Center, were not in a place where they would have a "reasonable expectation of privacy." Id. Finding that such expectations normally exist in bedrooms, bathrooms, changing rooms, tanning rooms, and the like, the Court held that the statute's language did not prohibit "up-skirt" photography in a public place, even though the statute defined a place where a person would have a reasonable expectation of privacy to include places "where a reasonable person would believe that he or she could disrobe in privacy, without being concerned that his or her undressing was being photographed" or "A place where one may reasonably expect to be safe from casual or hostile intrusion or surveillance." Id. at 150-151 (emphasis added). The Court reasoned that public places could not logically constitute locations in which a person could "reasonably expect to be safe from casual or hostile intrusion or surveillance." Id. at 150. In sum, the Court interpreted the unambiguous language of the statute as being focused on the location of the conduct at issue, and not the part of the person's body being photographed. Id. The Court noted the frustration of states with technologically-enhanced voyeurism, and noted statutes in California and Louisiana that protect identifiable victims of so-called "up-skirt" photography by statutory language focusing on the unreasonable and offensive nature of the actor's conduct, rather than the location of the intrusion. Id. at 151. California's revised statute, for example, refers to "circumstances," not merely places, in which a victim has a reasonable expectation of privacy. Id. at 152. For excellent treatments of the issue of privacy and acts of voyeurism employing imaging technology, see Lance E. Rothenberg, Re-Thinking Privacy: Peeping Toms, Video Voyeurs, and the Failure of Criminal Law to Recognize a Reasonable Expectation of Privacy in the Public Space, 49 Am. U. L. Rev. 1127 (2000), and David D. Kremenetsky, Insatiable "Up-skirt" Voyeurs Force California Lawmakers to Expand Privacy Protection in Public Places, 31 McGeorge L. Rev. 285 (2000).

^{105.} N.Y. Assembly 8115, 22d Leg., 1999–2000 Reg. Sess. (Apr. 29, 1999).

2003] CCTV and Other Video Security Technology

assist the state police in reducing alcohol-related traffic accidents. 106

C. Summary of Constitutional and Privacy Issues

Burrows suggests that serious consideration must be given to the argument that extending expectations of privacy to public places to preclude video surveillance will, in fact, impede law enforcement efforts to protect the public from crime. He observes that many citizens support public surveillance programs, so long as they comply with the need to prevent abusive use of the technology or videotapes. He advises, however, that the warrantless use of video surveillance by police should be limited to public streets, where the Supreme Court has held that citizens have no reasonable expectation of privacy. Burrows emphasizes that the right of privacy is a fundamental right in our society and that the more than 600,000 state and federal law enforcement personnel, and 1.5 million private security personnel, with resources in excess of thirty billion dollars, present a force that has already eroded notions of privacy once taken for granted. He given to public streets and privacy once taken for granted.

Additionally, both legal writers and journalists express concern that police may use video surveillance to "target" minorities who are stereotyped as likely to commit crimes, as well as members of unpopular political action groups in the community. Most importantly, writers on the subject caution that, in our efforts to reduce crime, we must not trade individual liberties for rigid notions of security, safety, or order. Technology should be used to support arrests only when it is reliable, and aspects of its unreliability or potential abuse must be understood and evaluated. Its

321

^{106.} R.I. Gen. Laws \S 42-28.9 (2000). These mounted video/audio surveillance cameras assist the police "in the exercise of their duties." Id.

^{107.} Burrows, supra n. 4, at 1123.

^{108.} Id. at 1124.

^{109.} Id.

^{110.} *Id.* at 1125–1126.

^{111.} $E.g.\ id.$ at 1126 (discussing video surveillance of minority groups, political "fringe" groups, and "subversive" organizations).

^{112.} E.g. id. ("The fact that law enforcement may be made more efficient is never by itself a justification to disregard the Constitution").

^{113.} See Burrows, supra n. 4, at 1127 (noting that digital imaging allows a criminal to be removed from a scene or placed at a scene, and that an expert might not be able to distinguish a copy from the original master tape). Burrows also expresses concern that

To achieve these objectives, the American Bar Association (ABA) has proposed standards for the use of video surveillance. These standards permit the use of video surveillance when it is "reasonably likely to achieve a legitimate law enforcement objective . . . approved by a politically accountable political official, and . . . presented to the public . . . [with] an opportunity for comment. In promulgating these standards, the ABA recognized that technology is rapidly evolving, and, for that reason, future modifications of the standards may be appropriate. It further recognized that the standards provide only a framework for analysis and do not address or resolve all conceivable issues that may arise. Nevertheless, the ABA Committee decided to publish the standards for three reasons:

First, technologically-assisted physical surveillance has become routine practice in some law enforcement contexts. . . . There is no doubt that such surveillance will continue to increase both in scope and in complexity. Some type of regulatory framework, even one that will require revision in the future, is needed. 118

Second, the courts have not developed such a framework and, to the extent the courts have acted, their decisions have not always been consistent. Finally, the ABA hoped that issuing the standards would prompt nonjudicial law-making in the area. In short, the ABA standards represent a considered effort to describe and balance the constitutional and privacy concerns that underlie the use of video surveillance systems with the legitimate needs of

citizens could access surveillance footage through the Internet on their personal computers. *Id.* Some jurisdictions are already establishing a structure for bringing together groups having competing concerns about the parameters of the use of video surveillance in targeted retail/commercial areas of the city. *See e.g. Agenda Report, City of Oakland, SIA Report* app. 9, 179–180 (but noting the decision not to seek opinion of City Attorney unless there is a governmental role in the surveillance program).

^{114.} ABA Crim. Just. Stands. Comm., ABA Standards for Criminal Justice: Electronic Surveillance, Section B: Technologically-Assisted Physical Surveillance 1–10 (3d ed., ABA 1999).

^{115.} Mark Hansen, If Crime Is Everywhere, So, Too, May Be Police Surveillance Cameras and Contraband Detection Devices to Combat It. But Who's Looking Out for Privacy Rights? 83 ABA J. 45, 48 (Aug. 1997).

^{116.} ABA Crim. Just. Stands. Comm., supra n. 114, at 5.

^{117.} Id. at 9.

^{118.} Id. at 5.

^{119.} Id. at 6.

^{120.} Id. at 7.

2003] CCTV and Other Video Security Technology

law enforcement agencies to better protect the safety and security of the public. 121

IV. EMPLOYER USE OF VIDEO SURVEILLANCE IN WORK AREAS

While much of the focus of the video surveillance debate has been in the context of law enforcement prerogatives in the general community, the issue of silent video surveillance has also been the subject of considerable interest in the workplace setting. Both the courts and the National Labor Relations Board (NLRB) have been exploring the issue, using essentially the same principle that has been articulated in the law enforcement context—the reasonable expectation of privacy. However, it is important in the workplace setting to keep in mind that the privacy analysis first depends upon whether the employer is public or private, because public employers are directly subject to Fourth Amendment protections against unreasonable searches and seizures. 122 In O'Connor v. Ortega, 123 the United States Supreme Court held that a physician employed by a state hospital had a reasonable expectation of privacy regarding the contents of his private office at the hospital. 124 The constitutionally protected expectation of privacy does not create a per se rule of constitutional law that protects any public employee's office space, but it does directly raise a constitutional question. 125 Private employers, on the other hand, are governed by common-law tort and contract constraints. 126

323

^{121.} The general principles standard suggests factors defining the balance, including the nature of the law enforcement objectives, the extent to which the surveillance will achieve those objectives, and the nature and extent of the crime involved, as compared with the nature of the place, activity, condition, or location to be subjected to surveillance, the care that has been taken to enhance the privacy interests suggested, the lawfulness of the vantage point and the sense enhancement capability of the technology being used, and whether the surveillance is overt or covert. *Id.* at 8–9.

^{122.} See O'Connor v. Ortega, 480 U.S. 709, 715 (1987) (stating, "Searches and seizures by government employers . . . are subject to the restraints of the Fourth Amendment").

^{123. 480} U.S. 709.

^{124.} Id. at 718.

^{125.} See id. at 719–720 (explaining that the employee's expectation of privacy must be balanced against "the government's need for supervision, control, and the efficient operation of the workplace").

^{126.} Frank C. Morris, Employment Discrimination and Civil Rights Actions in Federal and State Courts: Privacy, Defamation and Intentional Infliction of Emotional Distress in Employment 770 (ALI–ABA CLE Course of Study, 2000).

Vega-Rodriguez v. Puerto Rico Telephone Co. ¹²⁷ is instructive in the public employer context. In Vega-Rodriguez, a quasi-public telephone company installed three cameras surveying the work-place and a fourth camera to view all traffic passing through the main entrance. ¹²⁸ The surveillance was exclusively visual. ¹²⁹ The company stored the videotapes, which could be viewed only with the permission of a designated company official. ¹³⁰ The employees objected to the cameras on the ground that the surveillance constituted an unreasonable search under the Fourth Amendment and, therefore, violated a constitutionally protected right to privacy. ¹³¹ When the company refused to remove the cameras, the employees filed suit. ¹³²

The First Circuit rejected this challenge, holding that unconcealed video surveillance in a worker's common area does not violate the worker's privacy rights. The court recognized that public employees may be protected against unreasonable search and seizure if the challenged conduct infringes a reasonable expectation of privacy. However, that protection must be both subjectively demonstrable and objectively reasonable under the circumstances. Generally, the employee's expectation of privacy is objectively reasonable as to his or her exclusive private office, desk, and file cabinets containing personal matters not shared with other workers. In contrast, there is no reasonable expectation of privacy against video surveillance of open work areas, unenclosed locker areas, or desks, files, and the like, which are subject to shared access among employees, especially when the employer discloses its use of surveillance. The *Vega-Rodriguez* court did

```
127. 110 F.3d 174 (1st Cir. 1997).
```

^{128.} Id. at 176.

^{129.} Id.

^{129.} *Id*. 130. *Id*.

^{131.} *Id*. at 177.

^{132.} Id.

^{133.} Id. at 180.

^{134.} *Id.* at 178 (citing *Oliver v. U.S.*, 466 U.S. 170, 177 (1984); *Smith v. Maryland*, 442 U.S. 735, 740 (1979)).

^{135.} Id.

^{136.} Id. at 179 (discussing O'Connor, 480 U.S. at 718-719).

^{137.} Id. at 179–180 (citing Sheppard v. Beerman, 18 F.3d 147, 152 (2d Cir. 1994); American Postal Workers Union v. U.S. Postal Serv., 871 F.2d 556, 560–561 (6th Cir. 1989); Schowengerdt v. U.S., 944 F.2d 483, 488 (9th Cir. 1991); Taketa, 923 F.2d at 673; O'Bryan v. KTIV TV, 868 F. Supp. 1146, 1159 (N.D. Iowa 1994); Thompson v. Johnson County Community College, 930 F. Supp. 501, 507 (D. Kan. 1996)).

325

not, however, close the door on all privacy concerns in the context of workplace surveillance. The court cautioned that "cases involving the covert use of clandestine cameras, or cases involving electronically-assisted eavesdropping, may be quite another story."138

This latter aspect of the First Circuit's opinion in Vega-Rodriguez was examined, in the context of both state and federal constitutional protection of privacy, in Cowles v. State. 139 In Cowles, a divided Alaska Supreme Court held that an employee of the University of Alaska had no objectively reasonable expectation of privacy that would prohibit the University's installation of a hidden video camera in the ceiling vent over her desk in the University's theater box office for the purpose of recording her theft of money. 140 A bare majority of the Court affirmed the employee's conviction of theft, based in part on the admission of a videotape showing her transfer of cash receipts from the theater cash bag to her desk and then to her purse. 141 The majority reasoned that such covert use of video monitoring was not inconsistent with either federal or state protections of privacy because, from a societal perspective, the employee's subjective expectation of privacy was not reasonable. 142

The majority held that neither the federal nor the Alaska constitutional protections against unreasonable searches and seizures subsumed those activities which a person knowingly exposed to the public—whether in his or her home or in his or her office. 143 Although the employee's office was, subjectively, an area in which she might not have expected to be secretly videotaped, her desk was, in fact, visible to the public through the ticket window and to her co-workers through the open office door; additionally, there was an almost continuous flow of traffic around her desk. 144 The open and public nature of the employee's work environment suggested that any expectation of privacy concerning her handling of University monies at and around her desk could not reasonably be sustained. 145

```
138. Id. at 180 n. 5.
```

^{139. 23} P.3d 1168, 1170 (Alaska 2001).

^{140.} Id. at 1175.

^{141.} Id.

^{142.} Id.

^{143.} Id. at 1171 (citing Katz, 389 U.S. at 351).

^{144.} Id. at 1170–1171.

^{145.} Id. at 1172-1173. The majority attached special importance to the fact that the

The Cowles majority distinguished both United States v. Taketa, 146 a decision of the Ninth Circuit Court of Appeals, and State v. Bonnell, 147 a Hawaii Supreme Court decision, involving arguably comparable issues of fact and law. 148 In Taketa, Drug Enforcement Administration (DEA) agents installed a hidden video camera, without a warrant, in the ceiling of an office used by an employee of the Nevada Bureau of Investigation (NBI). 149 The Ninth Circuit found the covert video surveillance unreasonable under the facts of the case. 150 The surveillance targeted the employee and his supervisor, a special agent in charge of the DEA suite in which the office was located. 151 The court noted that "even 'private' business offices are often subject to the legitimate visits of coworkers, supervisors, and the public, without defeating the expectation of privacy unless the office is 'so open to fellow employees or the public that no expectation of privacy is reasonable." Applying O'Connor, the Taketa court found that the targeted office was not open to the public and was not regularly visited by DEA agents. 153 The only people with regular access to the office were the agents stationed at the airport.¹⁵⁴ The agents' access did not defeat the employee's subjective expectation of privacy, nor did it compromise the reasonableness of that expectation under Katz, because the office was assigned to the employee for his exclusive use. 155

The employer in *Bonnell* installed the covert video camera in a post-office employee break room in cooperation with the Maui

case involved an employee with custodial responsibility for public monies, suggesting that when a public employee occupies a job with high security requirements, it is less reasonable for her to assume that her on-the-job conduct will be private. *Id.* at 1173.

- 146. 923 F.2d 665 (9th Cir. 1991).
- 147. 856 P.2d 1265 (Haw. 1993).
- 148. Cowles, 23 P.3d at 1173-1174.
- 149. 923 F.2d at 668-669.
- 150. Id. at 677.
- 151. Id.
- 152. Id. at 673 (quoting O'Connor, 480 U.S. at 717-718).
- 153. Id.
- 154. Id.

^{155.} Id. The court held that "the video surveillance was not an investigation of work-related employee misconduct that could benefit from the reasonableness standard of O'Connor." Id. at 675. Moreover, the court held that the employee targeted by the hidden camera had a reasonable expectation of privacy because he, and not the property, was the subject of the surveillance. Id. at 677. The court emphasized that the constant videotaping was more intrusive than a singular entry into the office. Id.

327

Police Department.¹⁵⁶ The purpose of the warrantless video surveillance was to detect employees' suspected gambling activities.¹⁵⁷ The Hawaii Supreme Court held that the defendants, as employees, had a reasonable expectation of privacy under the state's constitution with regard to their activities in the employee-only break room, which was not a public place or a place subject to public view or public visitation.¹⁵⁸ In a statement suggesting its opposition to the kind of narrow distinctions relied upon by the *Cowles* Court, the Hawaii Supreme Court observed that,

"[t]he showing of necessity needed to justify the use of video surveillance is higher than the showing needed to justify other search and seizure methods, including bugging. The use of a video camera is an extraordinarily intrusive method of searching.... Because of the invasive nature of video surveillance, the government's showing of necessity must be very high to justify its use." ¹⁵⁹

Considering the issue left partly open in *Vega-Rodriguez*, the majority in *Cowles* held that the fact that the University hid the camera in a ceiling vent and installed it for the specific purpose of targeting the employee—following another employee's reported suspicion that she was stealing box office monies—did not create an expectation of privacy. The Court explained that, when a public employee engages in incriminating conduct in a public area, she risks observation and has no right to demand that such observation be by a person or technology of which the employee is aware. Having said this, the majority did suggest constitutional

^{156. 856} P.2d at 1270.

^{157.} Id.

^{158.} *Id.* at 1277. The Court affirmed the suppression of videotaped footage of a few minutes of employees' gambling activities in the break room. *Id.* at 1279. There were more than 1,200 hours of continuous and warrantless videotaping of the employees in the break room, obtained using a hidden video camera placed there for the purpose of the Maui Police Department's criminal investigation. *Id.* at 1270–1271. The Court held that, given the yearlong duration of the taping, the State had no argument that exigencies precluded the obtaining of a warrant. *Id.* at 1273.

^{159.} *Id.* at 1273 n. 5 (quoting *Mesa-Rincon*, 911 F.2d at 1442–1443); *see also Brannen v. Kings Local Sch. Dist. Bd. of Educ.*, 761 N.E.2d 84, 91–92 (Ohio App. 12th Dist. 2001) (rejecting custodians' claim of privacy in break room on the ground that it was, in fact, an all-purpose utility room teachers and other school employees used, which was also open to administrative personnel).

^{160.} Cowles, 23 P.3d at 1172.

^{161.} *Id.* The Court rejected the majority holding in *State v. Thomas*, 642 N.E.2d 240 (Ind. App. 1994), which upheld the suppression of a covert videotape of the activities of a

limitations on the covert video monitoring of public employees, even in public access areas, when there is no established legiti-

[Vol. XXXIII

mate purpose or reasonable cause for the use of hidden cameras.¹⁶² The dissent in Cowles suggested a compelling constitutional analysis, consistent with United States Supreme Court precedent

and the emerging law of the few states that have considered the covert use of video monitoring in the workplace. 163 The dissent fundamentally disagreed with the majority's interpretation and application of both Katz and O'Connor, and suggested that both federal and state constitutional law should protect an employee from the warrantless use of hidden video cameras in any area of the workplace not subject to general public access. 164 More specifically, the dissent characterized the majority's view of Katz—as limiting search and seizure protections to private locations—as

defendant licensee who operated a state park store under an agreement requiring him to pay ten percent of his gross receipts to the state. Id. at 247. The court of appeal held that, under the concession agreement, the defendant had a possessory interest in the store and in his own money—and thus, an expectation of privacy which prohibited the use of a hidden video camera for the purpose of recording his handling of receipts. Id. at 245. The Cowles majority agreed with the dissenting judge in Thomas that, because the videotaped transactions were open and visible to the public, there was no reasonable expectation of privacy attaching to defendant's activities. Cowles, 23 P.3d at 1175.

162. Id. at 1175. The majority specifically limited its conclusion that the University's actions were constitutionally permissible, stating that this conclusion would not necessarily have been the same if the monitoring had not been initiated based upon reasonable grounds to believe that the employee was engaged in the theft of box office receipts. Id. The Court noted that, "[1]acking a legitimate purpose, or reasonable cause, the utility of the monitoring would be diminished and a different balance might be struck." Id. The two dissenting justices rejected the majority's limitations of privacy protections to "private offices," suggesting that workers have objectively reasonable expectations of "privacy from surreptitious police surveillance regardless of the nature of their work space." Id. (Fabe & Bryner, JJ., dissenting). Reading the Court's prior decision in State v. Glass, 583 P.2d 872 (Alaska 1978), as expressing "grave concerns about electronic surveillance technologies and their effect on 'the right of persons to determine for themselves when, how, and to what extent information about them is communicated to others," the dissent suggested that constitutional limitations on warrantless video monitoring should be comparable to the limitations imposed on audio surveillance. Cowles, 23 P.3d at 1176-1177 (quoting Glass, 583 P.2d at 880). Indeed, the dissenters argue that Glass implies that protection from electronic surveillance extends to people in public places. Id. at 1177 n. 19 (citing, with approval, both Bonnell, 856 P.2d 1265, and State v. Brackman, 582 P.2d 1216 (Mont. 1978)).

163. See Cowles, 23 P.3d at 1175 (Fabe & Bryner, JJ., dissenting) (arguing that the majority decision "disregards ample state and federal precedent that workers should expect privacy from surreptitious police surveillance regardless of the nature of their work

164. See id. at 1178-1179 (discussing the majority's interpretation of Katz and O'Connor).

2003]

CCTV and Other Video Security Technology

wrong. ¹⁶⁵ The dissenters captured the rule of law more fully than the majority: "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, *even in an area accessible to the public*, may be constitutionally protected." ¹⁶⁶ Perhaps more compelling, the dissenters argued that the plurality opinion of the *O'Connor* Court must be read as holding that the *Katz* standard prohibits the general compromise of an employee's constitutional privacy rights merely because his or her office is open to other employees in the conduct of the employer's business. ¹⁶⁷

In the private employer setting, the focus of the discussion turns mainly on common law tort "invasion of privacy" analysis and, in the union context, on collective bargaining principles. The Seventh Circuit's opinion in *Brazinski v. AMOCO Petroleum Additives Co.*¹⁶⁸ presents a thought-provoking discussion of the tensions between employee expectations of privacy and employer concern for employee misconduct when private employment rights are in dispute.

In *Brazinski*, eight female workers at an AMOCO chemical laboratory challenged, in state court, their employer's installation of a television camera in the ceiling of a locker room used by female employees to change from their street clothes into work clothes. The company explained that it installed CCTV to document improper—presumably sexual—activity by a certain male employee and a certain female employee in the locker room during working hours. However, seeking to avoid a determination

329

^{165.} Id. at 1178.

^{166.} Id. (quoting Katz, 389 U.S. at 351 (emphasis in original)).

^{167.} *Id.* The dissenters note that *O'Connor* must be read in the context of Justice Antonin Scalia's concurring opinion and his explicit conclusion that a secretary working in an office frequented by other employees does not lose constitutional privacy protections because of the restricted access permitted, but rather loses those protections only under circumstances that suggest the office is subject to unrestricted public access. *Id.* at 1178–1179. The dissent's reading of *Bonnell* and *Taketa* as holding that an employee has a reasonable expectation of privacy in some areas of his or her workplace—even when those areas may be accessed by other employees—is clearly an accurate reading of those cases. *See Bonnell*, 856 P.2d at 1276 (holding that an employee's expectation of privacy in some area of the workplace "is not defeated merely because the area is accessible to others" (citing *Taketa*, 923 F.2d at 673)).

^{168. 6} F.3d 1176 (7th Cir. 1993).

^{169.} Id. at 1178, 1182.

^{170.} Id. at 1182.

of the merits, the company argued that the suit implicated the company's collective bargaining agreement with the plaintiffs' union and, thus, was a suit under Section 301 of the Taft-Hartley ${\rm Act.}^{171}$

The employer successfully removed the case to federal district court, and the court entered summary judgment in favor of the company because the plaintiffs failed to file a grievance under the bargaining agreement. Affirming the summary judgment against the union plaintiffs, the Seventh Circuit nonetheless rendered an opinion on the supplemental claim of one non-union plaintiff that the company's use of CCTV in the female employees' locker room subjected her to being taped in a state of undress. 173

The court observed that state tort law might support a claim that,

[a] well-motivated but unavoidably indiscriminate effort at [video] surveillance is actionable on behalf of a person, [who is] not the target of the surveillance, [but] who accidentally wanders onto the scene and is photographed or recorded [in a state of undress].¹⁷⁴

The court cautioned, however, that "if the method of surveillance chosen is the least indiscriminate possible for achieving a lawful and important objective, the stranger whose privacy is incidentally and accidentally compromised" might not have a cause of action. ¹⁷⁵ If a cause of action were to be recognized, the court observed, the plaintiff would be required to demonstrate that she was seen by a live human being—either a person monitoring the camera or viewing the tape—or, at the very least, that she was in the place under surveillance so that, if the equipment was manned, she would have been seen or heard. ¹⁷⁶

^{171.} Id. at 1178.

^{172.} *Id*

^{173.} *Id.* at 1183. The non-union plaintiff was, in fact, an electrician employed by another company but engaged in work on the defendant's premises. *Id.* at 1181.

^{174.} Id. at 1183.

^{175.} Id. The court noted that this situation could arise, for example, when an innocent person visits an apartment that is under police surveillance. Id.

^{176.} *Id.* The employer argued that the camera was aimed, at all times, at the entry door to the locker room. *Id.* at 1184. Finding that the plaintiff introduced no evidence that she was in the locker room during the periods of CCTV surveillance or that the camera was aimed inside the locker room, the court affirmed the dismissal of the complaint. *Id.*

2003] CCTV and Other Video Security Technology

More recently, the Ninth Circuit addressed the issue of private workplace surveillance in Cramer v. Consolidated Freightways, Inc. 1777 In Cramer, the defendant trucking company installed video cameras in the terminal restrooms as part of an effort to detect and deter drivers' drug use. 178 The plaintiff employees, alleging invasion of privacy and infliction of emotional distress, sued in state court seeking damages and an injunction. ¹⁷⁹ The employer, like the employer in *Brazinski*, removed the case to federal court on the ground that all claims fell within the preemptive reach of Section 301 of the Labor Management Relations Act. 180 The employer then moved to dismiss on the same basis.¹⁸¹ In upholding the employer's position, the court reasoned that expectations of privacy in the workplace could not be analyzed without considering the collective bargaining agreement. 182 The collective bargaining agreement governed working conditions of employment, and video surveillance—a working condition—is a matter of contract between labor and management.¹⁸³ Thus, the question of whether an employee had a reasonable expectation of privacy, and whether that expectation was violated, depended, at least in part, on the terms of the collective bargaining agreement. 184 The state law tort claims for invasion of privacy were, accordingly, preempted by federal labor law. 185

The NLRB also has opined on this subject. In *Colgate-Palmolive Co. & Local 15*, *International Chemical Workers Union*, ¹⁸⁶ it ruled that the installation of video surveillance cameras in the workplace should be considered "a mandatory subject of bargaining." The underlying incident in the case involved an employee who, while cleaning a restroom at the workplace, looked up and observed a camera, about six to eight feet away, angled toward him. ¹⁸⁸ He had been unaware of the company's use of sur-

```
177. 209 F.3d 1122 (9th Cir. 2000).
```

331

^{178.} Id. at 1127.

^{179.} Id.

^{180.} Id.

^{181.} Id.

^{182.} Id. at 1130.

^{183.} Id. at 1131.

^{184.} Id.

^{185.} Id. at 1133.

^{186. 323} N.L.R.B. 515 (Natl. Lab. Rel. Bd. 1997).

^{187.} Id. at 515.

^{188.} Id. at 517.

veillance cameras and informed the union.¹⁸⁹ The union then made a request to bargain over the installation of the surveillance cameras; the company refused.¹⁹⁰ The NLRB, in concluding that video cameras are a mandatory subject of bargaining, found that cameras are investigatory tools, like physical examinations, polygraph testing, and drug testing, all of which the NLRB has held to be mandatory subjects of bargaining.¹⁹¹ The NLRB further held that the installation of hidden surveillance cameras should not be considered "a managerial decision that lies at the core of entrepreneurial control."¹⁹² In other words, the NLRB has recognized the employee's fundamental privacy interests as a critical component of an employee's working conditions and, since video surveillance implicates these privacy concerns, it cannot be unilaterally imposed on the workforce by the employer.

While these decisions provide a measure of protection for employees, they simultaneously suggest that employers may ultimately have significant control over workplace surveillance use. Employers enjoy this control because they can promulgate workplace policies in a non-union environment, or negotiate agreements with a unionized workforce, that change the employees' reasonable expectations of privacy. If workplace policies or agreements permit the use of hidden video surveillance, and the use of video surveillance is determined to serve a legitimate business interest, employees may be precluded from asserting privacy claims to bar the use of the technology.

^{189.} Id.

^{190.} See id. at 518 (explaining that the company did not respond to the union's request).

^{191.} Id. at 515.

^{192.} Id.

^{193.} See Lawrence E. Rothstein, *Privacy or Dignity? Electronic Monitoring in the Work-place*, 19 N.Y.L. Sch. J. Intl. & Comp. L. 379, 405 (2000) (stating, "As the employer has the right to manage the employee for the employer's business purposes, there is little that the employee has a right to keep private if it impinges in any way on the workplace").

^{194.} See id. (explaining how an employer can "unilaterally change" employee expectations by instituting certain policies "or by simply intruding on one or more occasions").

^{195.} Frank Morris identifies the following factors as relevant to determining whether an employer's use of video surveillance has violated the employee's reasonable expectation of privacy: (1) whether the surveillance serves a legitimate business interest like safety or security; (2) whether the cameras are located in places where an employee might have a reasonable expectation of privacy, such as a restroom; (3) whether the cameras are visible; (4) whether employees are informed of the surveillance before accepting the job; (5) whether the employer is private or public; (6) whether a specific crime is being investigated; (7) whether the surveillance targets only protected groups; (8) whether the surveil-

Moreover, union activity itself receives special protection from video surveillance under Section 158(a)(1) of the National Labor Relations Act. 196 Recent cases like *California Acrylic Industries, Inc. v. National Labor Relations Board* 197 hold that, in the absence of proper justification (e.g., violence or trespass), the videotaping of union pickets or union/employee activity during organizing efforts or contested elections has a tendency to intimidate and interfere with the employees' right to engage in concerted activity. 198 In *California Acrylic*, the court specifically held that an employer may not videotape such activities on the basis of an undifferentiated fear that "something might happen." 199 Even if the employer's videotaping is justified as a lawful precaution against violence, the employer must be careful not to exceed the necessary boundaries of surveillance activities.

V. TORT CLAIMS AND VIDEO SURVEILLANCE

A. Negligence Principles

Modern tort law has been increasingly concerned with the security of premises, but modern rules both expand and limit duty.

lance is limited to work-related activities; and (9) whether state statutes or constitutional provisions are implicated. Morris, supra n. 126, at 772–773.

- 196. 29 U.S.C. § 158(a)(1) (2000).
- 197. 150 F.3d 1095 (9th Cir. 1998).
- 198. *Id.* at 1099–1100.

199. *Id.* at 1100; see also Clock Electric, Inc. v. NLRB, 162 F.3d 907, 918 (6th Cir. 1998) (holding that a company was not justified in photographing a picketing employee based on the mere belief that there might be a secondary boycott); Natl. Steel & Shipbldg. Co. v. NLRB, 156 F.3d 1268, 1271 (D.C. Cir. 1998) (discussing possible justifications for video surveillance that would mitigate its tendency to coerce); cf. Overnite Transp. Co. v. NLRB, 140 F.3d 259, 264–266 (D.C. Cir. 1998) (holding that videotaping by employees, who were union supporters but not union members, did not violate the Act when the employer could not show that their activities should be attributed to the union under common-law agency principles).

Where election misconduct is attributable to one of the parties, the Board will overturn the election if the misconduct created such an environment of tension and coercion as to have had a probable effect upon the employees' actions at the polls and to have materially affected the results of the election.... Where misconduct is attributable to third parties, however, the Board will overturn an election only if the misconduct is so aggravated as to create a general atmosphere of fear and reprisal rendering a free election impossible.

Overnite Transp. Co., 140 F.3d at 264–265 (internal quotations and citations omitted). 200. See Horsehead Resource Dev. Co. v. NLRB, 154 F.3d 328, 341 (6th Cir. 1998) (holding that surveillance, which went beyond taping access to the front gate to surveillance of union members who were in no way engaged with company employees or property, was unjustified).

In most, if not all, jurisdictions, courts or legislatures originally announced modern duty rules to limit the "old" common-law's imposition of strict liability on innkeepers for the loss or destruction of a guest's personal property. However, in modifying the "old" common-law rule, modern courts have imposed a duty on landowners to exercise reasonable care for the safety of business or public invitees. Page 2012

The modern rule provides that a landowner who holds land open to the public is subject to liability for physical harm to invitees "caused by the accidental, negligent, or intentionally harmful acts of third persons. . ." if the landowner fails to use reasonable care to (a) discover that such acts are occurring or are likely to occur, or (b) adequately warn visitors to avoid such harm or otherwise protect them from it. Decause the rule derives from negligence (fault) principles, and not strict liability theory, liability is "pegged" to foreseeability of harm. Additionally, because the landowner is not generally required to anticipate that third parties will commit criminal acts, the landowner is subject to liability only when criminal intrusion is reasonably foreseeable. Decause the

The rule is usually stated to provide that the landowner (e.g., landlord) may be negligent, even though the harm to a visitor/invitee (e.g., tenant) is caused by the criminal act of a third person, if the situation is one in which a reasonable landowner would have foreseen the likelihood of criminal intrusion. The landowner/proprietor is not the insurer of the invitee's safety, but must exercise reasonable care to protect the invitee from unreasonable risks of which the landowner has superior knowledge. Description of the invited of the inv

What constitutes reasonable care in a given situation varies with the circumstances, but generally, "evidence of substantially similar prior criminal acts" can be used to demonstrate that the landowner had actual or constructive knowledge of a risk of harm

^{201.} See e.g. Kutbi v. Thunderloin Enter., Inc., 698 P.2d 1044, 1046 (Or. App. 1985) (stating, "This statute and its predecessors were enacted to modify the common law's imposition of strict liability on innkeepers for loss or damage to a guest's personal property" and citing McIntosh v. Schops, 180 P. 593, 593 (Or. 1919)).

^{202.} See Restatement (Second) of Torts $\$ 344 (1965) (addressing business premises open to the public).

^{203.} Id.

^{204.} Id. at cmt. f.

^{205.} See id. at § 302 (defining a "negligent act" or "omission").

^{206.} Shoney's, Inc. v. Hudson, 460 S.E.2d 809, 811 (Ga. App. 1995), overruled in part on other grounds, Brown v. State, 549 S.E.2d 107 (Ga. 2001).

2003] CCTV and Other Video Security Technology

to the invitee.²⁰⁷ The term "substantially similar" does not mean identical—as, for example, whether a weapon was used—but whether the prior crimes would put a reasonable landowner on notice that invitees were subject to an increased risk of harm.²⁰⁸ The question is whether the prior activity would have attracted the attention of a reasonably prudent landowner and caused him or her to be concerned about the safety of visitors, tenants, etc.²⁰⁹

The general character of the event or harm must be foreseeable, not the precise nature of the activity or the precise manner of its occurrence. The California Supreme Court has suggested that not all cases require a showing of prior acts as a precondition to a finding that criminal activity was foreseeable. In *Isaacs v. Huntington Memorial Hospital*, a doctor sued the hospital for damages when a gunman assaulted him in a "research" parking lot across the street from the hospital's emergency room and physicians' entrance. The trial court granted the hospital's motion for nonsuit at the close of the plaintiff's case, finding insufficient evidence to hold the hospital liable for negligence. The California Supreme Court overturned the trial court's decision, holding, *inter alia*, that prior similar incidents are not a rigid requirement in finding that a landowner should have foreseen the risk of criminal behavior endangering invitees on its premises.

^{207.} Id.

^{208.} Id.

^{209.} *Id.*; *Cohen v. Southland Corp.*, 203 Cal. Rptr. 572, 575 (Cal. App. 4th Dist. 1984) (citing cases from Massachusetts, New Jersey, New York, North Carolina, Oregon, Pennsylvania, and Texas).

^{210.} Cohen, 203 Cal. Rptr. at 577; but see Boren v. Worthen Natl. Bank of Ark., 921 S.W.2d 934, 941–942 (Ark. 1996) (holding that a bank is not required to provide security at ATMs and that the fact that apartments or businesses are located in high crime areas does not, in itself, establish a duty to provide security). In Boren, the dissent argued that the Court should have adopted the foreseeable risk rule and also observed that it should be a question of fact whether the installation of cameras or other measures would have deterred the criminal acts causing the plaintiff's injuries. Id. at 942–943 (Brown, J., dissenting)

^{211.} See Isaacs v. Huntington Meml. Hosp., 695 P.2d 653, 659 (Cal. 1985) (stating, "Prior similar incidents are helpful to determine foreseeability but they are not necessary").

^{212.} Id

^{213.} Id. at 655. As the doctor opened the trunk of his car, a gunman grabbed him from behind, and then, as the doctor turned around, the gunman shot him in the chest. Id. The doctor sustained serious injuries and lost a kidney. Id.

^{214.} Id. at 657.

^{215.} Id. at 659, 662.

The Court held that a rigid rule discourages landowners from taking sufficient measures to protect premises they know are dangerous. However, such a requirement encourages "arbitrary results and distinctions" because there is uncertainty as to when the prior acts must have occurred or how near the acts must be to the premises in question. Finally, a "prior similar incidents" rule deprives the jury of its proper role in determining whether a reasonably prudent landowner would have determined that the risk of criminal assault was sufficiently evident to require security measures. In sum, the Court held that, while evidence of prior similar acts is helpful to a determination of foreseeability, it is not a "but for" requirement.

Balanced against the consideration of the likelihood and severity of harm to visitors, tenants, etc., is the burden to the landowner if he or she is required to eliminate or reduce the risk of harm. When reasonable efforts to reduce risk would not place an onerous burden on the landowner, it is more likely that he or she will be asked to take affirmative steps to reduce the risk of criminal activity that threatens visitors, tenants, etc. 221

^{216.} Id. at 658.

^{217.} Id. at 658-659.

^{218.} Id. at 659.

^{219.} Id. The Court observed that "[w]hether a given criminal act is within the class of injuries which is reasonably foreseeable depends on the totality of the circumstances and not on arbitrary distinctions." Id. at 659-660 (quoting Kwaitkowski v. Super. Trading Co., 176 Cal. Rptr. 494, 497 (Cal. App. 1st Dist. 1981)). A court may consider such factors as the nature and location of the premises, the access that strangers might have to the premises, existing security, lighting, etc., as well as prior criminal activity. See id. at 661-662 (discussing the location of the parking lot, as well as security and lighting of the parking lot, and concluding that there was sufficient information to provide notice of the risk of an assault). Thus, in Cohen, the court properly found that "the very operation of an all night convenience store . . . may be said to . . . [create] 'an especial temptation and opportunity for criminal misconduct,' thus increasing the foreseeablility of injury" to customers. 203 Cal. Rptr. at 578 (quoting William Prosser, Torts § 33, at 174 (4th ed., West Publg. Co. 1971)). Similarly, the operation of a parking garage in an office building located in a highcrime neighborhood raises a question of fact regarding the foreseeability of criminal assault, notwithstanding the plaintiff's inability to prove specific instances of prior assault on the premises. Gomez v. Ticor, 193 Cal. Rptr. 600, 606 (Cal. App. 2d Dist. 1983).

^{220.} Cohen, 203 Cal. Rptr. at 578.

^{221.} See Isaacs, 695 P.2d at 658 (explaining that when the burden of preventing future harm is low, a lesser degree of foreseeability is needed to impose a duty of reasonable care upon a landowner and citing *Gomez*, 193 Cal. Rptr. at 604); *Cohen*, 203 Cal. Rptr. at 579 (explaining that imposing a duty on a convenience store owner to take reasonable precautions to reduce the risk of early morning robberies does not place an onerous burden on the defendant because the store could simply make sure the parking lot is well lit).

To summarize, until recently, courts have been reluctant to impose liability on the owner of premises for injuries to the land-owner's invitees, tenants, customers, students, or others caused by the criminal acts of third parties. However, recently many courts have extended negligence rules to hold supermarkets, restaurants, libraries, schools, summer camps, and other entities liable for crime-related injuries. Even though the criminal act is, in fact, an intervening act, the landowner's antecedent negligence subjects him or her to liability if the criminal act was itself reasonably foreseeable. 223

B. Application of Negligence Principles in the Context of Video Surveillance

1. Failure to Utilize a Video Security System

A natural aspect of a modern negligent security claim is that a landowner's security system does not include available, cost-effective, and popularly utilized video surveillance equipment.²²⁴ In tort law cases, a plaintiff may actually introduce evidence of the "industry standard" to show negligence.²²⁵ Although departure from the "industry standard" does not establish negligence *per se*, the benchmark is relevant and admissible.

In *Nebel v. Avichal Enterprises, Inc.*, ²²⁶ a motel patron alleged that the defendant's employees were negligent in failing to provide "functional and operational closed circuit surveillance cameras and monitors," in a motel located in a well-known, high-crime area of Atlantic City, New Jersey. ²²⁷ The court held that, in cases alleging inadequate security, the plaintiff's obligation is to

^{222.} Nebel v. Avichal Enter., Inc., 704 F. Supp. 570, 572 n. 1 (D.N.J. 1989).

^{223.} Id. at 576. There is one important limit to this liability—because the allegation of negligent security in such situations is based upon the invitee's status and relationship with the landowner, the landowner's liability does not extend beyond his or her premises, and liability on the premises extends only to areas within the landowner's control. Id. at 577. Thus, for example, a landlord's duty to provide reasonable security to his or her tenants extends to those areas of the landlord's premises over which the landlord retains control during the lease, including common entrances, stairwells, laundry rooms, and recreation facilities.

^{224.} See e.g. id. at 572–573 (discussing plaintiff's contention that the defendant's "failure to employ at least some of the myriad security devices and techniques available to them" contributed substantially to the risk of crime).

 $^{225. \ \ \}textit{Fidalgo v. Columbus McKinnon Corp.}, 775 \ \text{N.E.2d } 803, 809 \ (\text{Mass. App. } 2002).$

^{226. 704} F. Supp. 570.

^{227.} Id. at 573.

prove that the defendant's negligence was a substantial factor causing the harm.²²⁸

Keeping in mind the basic rule of law that while the criminal act is, in fact, an intervening act, the defendant remains liable if the criminal act was foreseeable and the defendant did not exercise reasonable care to reduce the risk of its occurrence, the plaintiff essentially needs to prove that a video surveillance system or other security measures would likely have deterred the criminal activity that caused the plaintiff's injury. Indeed, the landowner cases may be the best illustration to date that the effectiveness of CCTV in reducing the likelihood of crime that threatens bodily safety is the central factor in establishing its legitimacy when privacy issues are not implicated.

The principle is addressed in *Morris v. Krauszer's Food Stores, Inc.*, ²³⁰ which upheld a jury award of damages when the plaintiff's estate introduced expert testimony that, considering the foreseeability of robbery, the defendant should have increased security measures, including the installation of video cameras. ²³¹

Isaacs is in accord.²³² In *Isaacs*, the California Supreme Court reversed a judgment of nonsuit, finding that the hospital's decision to disarm its security guards, the stationing of the guards far from the parking lot where the plaintiff was assaulted, dim lighting in the parking lots, and inadequate video monitoring of the parking lot areas created triable negligence issues.²³³

^{228.} *Id.* at 578–579. In clarifying the meaning of "substantial factor" in negligent security cases, the court explained that "the best that a plaintiff can do . . . is to prove that certain security devices or techniques, had they been implemented, would have reduced the *risk* of harm." *Id.* at 578 (emphasis in original).

^{229.} *Id.* at 580. The court's opinion contains a detailed discussion of the law of proximate causation, which need not be detailed here, but is instructive to the attorney or landowner who desires an in-depth discussion of the "significant factor" analysis that underlies the proximate cause theory in cases involving two or more alleged causes of harm.

^{230. 693} A.2d 510 (N.J. Super. App. Div. 1997).

^{231.} *Id.* at 515. The plaintiff's expert testified that the defendant should have installed a clearly visible closed-circuit television camera focused on the area of the cash register, as well as a barrier to protect the employees. *Id.* at 514.

^{232. 695} P.2d 653.

^{233.} *Id.* at 656, 663. The plaintiff's evidence included testimony from two security experts that, in light of the size of the premises, these deficiencies, as well as the lack of a communication protocol with local police, supported their opinion that the hospital's security was "totally inadequate" on the night the plaintiff was shot. *Id.* at 656.

2003]

CCTV and Other Video Security Technology

2. Use of Video Surveillance to Replace Security Guards or Officers

Although the cases are few in number, some observations may be made about the "reasonableness" of using silent video surveillance to replace or enhance security personnel, guards, and officers. In Shoney's, Inc. v. Hudson, 234 an assailant robbed and injured a patron in the parking lot of the defendant's restaurant.235 The patron alleged that the defendant knew of at least four acts of violence at that location within the past two years, including one shooting of a cashier. 236 The patron then alleged that the defendant initially responded by hiring security personnel during all evening hours, but later discontinued the use of guards and installed silent video cameras near the cash register of its new restaurant, which was located next to the old restaurant.²³⁷ Later, the defendant apparently hired guards to observe the premises on Friday and Saturday nights and to escort any employees who had bank deposits through the parking lot.²³⁸ Noting that the restaurant was located in the highest crime area of any of the defendant's establishments in Savannah, and that the defendants had acknowledged the potential for criminal attacks, the court held that the plaintiff raised an issue of material fact as to whether the defendant provided reasonable security for patrons. 239

The opinion can be read to state that a business or public invitee may allege that a landowner (e.g., storeowner, landlord, school) is negligent in discontinuing the use of security personnel and replacing them with silent video when the video is ineffectively deployed or located, or when reasonable care calls for the use of security guards or officers. Certainly, the court's opinion cautions, even if indirectly, against the undifferentiated use of video to replace security personnel merely to save money.

^{234. 460} S.E.2d 809.

^{235.} Id. at 810.

^{236.} Id. at 811.

^{237.} Id.

^{238.} Id.

^{239.} Id. at 812.

Stetson Law Review

[Vol. XXXIII

3. Policies, Procedures, and Employee Training

As *Cohen v. Southland Corp.* ²⁴⁰ illustrates, when devices are installed as the only security measure or to enhance security, the landowner must also be careful to follow its own policies regarding the installation and use of the technology. ²⁴¹ In *Cohen*, the defendant corporation commissioned a study of its store security and embarked on a program of employee security training and other security measures, like balancing the lighting inside and outside of the stores. ²⁴² When a robber shot a patron—while the store clerk hid in the back room of the store—the patron alleged that the installation of a security camera at the cash register did not represent adequate security unless store employees were adequately trained and store interiors and parking lots were properly illuminated. ²⁴³

4. False Sense of Security

Kutbi v. Thunderlion Enterprises, Inc. 244 suggests that the victims of a robbery or an assault might also allege negligence if there is evidence that a video security system is improperly designed or maintained, or is not monitored. The latter allegation may actually include a claim that a video security system, represented as monitored, but in fact not monitored, creates a false sense of security, thereby encouraging visitors, tenants, customers, and students to take risks they would not take if they knew the video security system was not monitored. 246

^{240. 203} Cal. Rptr. 572.

^{241.} See id. at 580 (finding that, although the defendant had instituted an elaborate training program, the store clerk working on the night of the incident in question had received no security training).

^{242.} *Id*. at 575.

^{243.} *Id.* at 574–575. Thus, where the plaintiff introduced evidence that the store manager had received no security training, despite the corporation's assertion that it had an extensive program of employee security training, and also introduced evidence of inadequate lighting on the night of the incident, summary judgement for the corporation was improperly granted. *Id.* at 580. The inference is, of course, that use of a video camera is not *per se* reasonable care when the situation demands additional forms of, or approaches to, security.

^{244. 698} P.2d 1044 (Or. 1985).

^{245.} See id. at 1047–1048 (holding that the trial court erred in granting summary judgment for the defendants because the plaintiff's "unrebutted allegations" presented issues of fact).

^{246.} See id. at 1047 (discussing plaintiff's allegations that the defendant used its video security system to lull patrons "into a false sense of security").

2003] CCTV and Other Video Security Technology

In *Kutbi*, the patron of a motor inn alleged that the defendant's employees were negligent, with respect to guest security, because they (1) duplicated an unreasonable number of excess keys; (2) maintained a video security system that was not in working order and that did not offer a view of the patrons' rooms; and (3) "lull[ed]" patrons "into a false sense of security" by not disclosing that the video security system was not regularly monitored. While the Court's opinion does not comment, in detail, on the plaintiff's third allegation, it implies that the defendant prevailed on this issue only because it introduced evidence that the security system was in good working order and was properly monitored on the night the plaintiff's room was burglarized. 248

5. Governmental Immunity

The "public duty doctrine" limits the liability of government landowners by generally precluding, under constitutional "separation of powers" analysis, a judicial imposition of executive branch policy. ²⁴⁹ In other words, a private plaintiff, who is a crime victim, could probably not obtain a private monetary award based upon the allegation that a public landowner (e.g., a university) generally devoted too few resources (too little budget) to safety and security. However, governmental agencies and entities should be cautious not to play "fast and loose" with this qualified immunity.

Where a visitor, tenant, or student enjoys a legal relationship with the landowner, the landowner's duty as landlord, premises operator, etc., makes it vulnerable to allegations of negligent security to the same extent that a private landlord/premises operator would be subject to liability. Indeed, in reality, except as to "undifferentiated" allegations of negligent security, the public institution, under most tort claims acts, is subject to liability to the

248. *Id.* at 1048. The Court denied the defendant's motion for summary judgement, finding that the plaintiff had introduced evidence sufficient to create a genuine issue of material fact on the questions of whether the defendant's employees had made excessive keys and had not changed the locks. *Id.*

^{247.} Id.

^{249.} Johnson v. State, 894 P.2d 1366, 1368 (Wash. App. Div. 1st 1995).

^{250.} See id. at 1370 (stating, "Under these circumstances, the relationship of this student to the university was sufficiently analogous to that of an invitee to justify imposing an equivalent duty of care upon the University").

extent it would be liable if it were a private entity.²⁵¹ While the line between policy-level and operational-level decision-making remains relevant for imposing liability on the governmental entity, it is possible to identify many aspects of the operation and use of a CCTV system that would likely be described as operational and, thus, subject to liability when protocols are violated.

C. Invasion of Privacy and Infliction of Emotional Distress

While landowners may be faced with tort claims based on the failure to employ video surveillance to protect tenants, customers, students, employees, and other invitees, they may concurrently face challenges under basic tort principles for the improper use of this same technology. Moreover, private tort law may be applied to the improper use of the technology in other contexts and environments.

There is a recognized tort for invasion of privacy, also known as "physical intrusion on solitude or private affairs." Salazar v. Golden State Warriors suggests that two elements are essential to this cause of action: "(1) intrusion into a private place, conversation, or matter, and (2) [intrusion] in a manner [that would be] highly offensive to a reasonable person." Salazar held that there was no invasion of privacy when a private investigator, hired by an employer, used an enhanced camera lens to film an employee, who was at all times in public view, to ascertain whether the employee was abusing drugs. To prove actionable intrusion, "the plaintiff must show [that] the defendant penetrated some zone of physical or sensory privacy"—it is not enough that the plaintiff has been observed, photographed, or recorded in a public place.

^{251.} E.g. Delaney v. U. of Houston, 835 S.W.2d 56, 63-64 (Tex. 1992).

^{252.} Salazar v. Golden State Warriors, 2000 U.S. Dist. LEXIS 2366 at *4 (N.D. Cal. Feb. 29, 2000).

^{253. 2000} U.S. Dist. LEXIS 2366.

^{254.} Id. at *4.

^{255.} *Id.* at **2, 7; see also Restatement (Second) of Torts, § 652B, cmt. c (1965) (discussing liability for observing a plaintiff in public).

^{256.} Salazar, U.S. Dist. LEXIS 2366 at *5. More recent intermediate court decisions suggest similar parameters in a variety of contexts. See e.g. Creel v. I.C.E. & Assoc., Inc., 771 N.E.2d 1276, 1281 (Ind. App. 2002) (rejecting plaintiff's claim of intrusion as an invasion of privacy). In Creel, the defendant's investigator, posing as a worshiper, used a hidden camera to videotape the plaintiff as she played the piano in front of her church congregation, as part of an investigation of her disability insurance claim. Id. at 1278. The intermediate appellate court affirmed summary judgment in favor of the defendant, hold-

The Supreme Court of California, for example, made clear, in *Shulman v. Group W Productions, Inc.*, ²⁵⁷ that there is no invasion of privacy when the plaintiff has no right of ownership or control of the premises where the incident took place. ²⁵⁸ In other words, the plaintiff must show that he or she had an objectively reasonable expectation of privacy.

Also, the invasion of privacy tort requires a showing that the intrusion would be viewed as "highly offensive to a reasonable person." California courts have restated the basic principle that "[v]ideo surveillance does not in itself violate a reasonable expectation of privacy," in Salazar and Sacramento County Deputy Sheriffs' Assn. v. County of Sacramento. Thus, in analyzing a claim for invasion of privacy for the use of video surveillance technology, courts will consider "the degree of intrusion, the context, conduct and circumstances surrounding the intrusion, as well as the intruder's motives and objectives, the setting into which he intrudes, and the expectations of those whose privacy is invaded."

ing that the plaintiff had no reasonable expectation of privacy in her activities when the investigator's secret videotaping simply recorded an activity that was open to the public and was observed by the more than 100 persons in attendance at the church service. *Id.* at 1281.

257. 955 P.2d 469 (Cal. 1998).

258. *Id.* at 490. The Court held that filming a rescue attempt at an accident scene off an interstate highway was not an invasion of privacy. *Id.*

259. Id. (citing Miller v. Natl. Broad. Co., 232 Cal. Rptr. 668, 678 (Cal. App. 2d Dist. 1986), and Restatement (Second) of Torts § 652B)).

260. 59 Cal. Rptr. 2d 834, 847 (Cal. App. 1st Dist. 1997) (holding that there was no offensive conduct to support a tortious privacy claim when a video camera was placed in a nonprivate office in a jail to observe possible criminal acts by deputy sheriffs).

261. Salazar, 2000 U.S. Dist. at *8. Worker's compensation claims cases may provide an additional context for evaluating tort claims based on intrusion of privacy. The theory has been most recently considered in this context in *I.C.U. Investigations, Inc. v. Jones*, 780 So.2d 685 (Ala. 2000). In *Jones*, the Alabama Supreme Court held that, in the absence of publication or commercial use, a plaintiff claiming wrongful intrusion into his or her private activities must present evidence that would permit a jury to conclude that the defendant's conduct outraged, or caused shame or humiliation to, a person of "ordinary sensibilities." *Id.* at 689. The Court reversed a jury award of damages to the plaintiff, was videotaped as he urinated in his front yard by a private investigator hired to perform surveillance in connection with the plaintiff's worker's compensation appeal. *Id.* at 687, 690. Three Justices dissented, reasoning that the activity in question was unrelated to the plaintiff's claim and that the plaintiff had a legitimate expectation of privacy, even in a "public place," because his act was not exposed to the public eye. *Id.* at 690–691 (Cook, Johnstone & England, JJ., dissenting).

The home seems to invite greater concern for privacy and emotional security. See Clayton v. Richards, 47 S.W.3d 149, 156 (Tex. App. Texarkana 2001) (holding that a hus-

Stetson Law Review

[Vol. XXXIII

In addition to the invasion of privacy tort, subjects of video surveillance may sue for intentional or negligent infliction of emotional distress. To prove a claim of intentional infliction of emotional distress, the plaintiff must show "(1) extreme and outrageous conduct by the defendant [made] with the intention of causing, or [with] reckless disregard for the probability of causing emotional distress, (2) [that the] plaintiff suffered severe or extreme emotional distress, and" (3) that the defendant's conduct was the proximate cause of the distress. Consent to the invasion of privacy will affect the court's determination of whether the defendant's conduct was outrageous. To prevail on a claim of negligent infliction of emotional distress, the plaintiff must show that the defendant breached some duty to protect the plaintiff's mental well-being. English in the defendant breached some duty to protect the plaintiff's mental well-being.

As applied to video surveillance, emotional distress claims may be more difficult to prove than claims for invasion of privacy. To succeed, a plaintiff must demonstrate a high level of emotional injury and a heightened degree of wrongful conduct by the defendant. Since courts are clear that video surveillance, by itself, does not constitute outrageous conduct to the extent that the defendant can justify its use for legitimate purposes, current case-law is slow to predict whether a plaintiff is able to establish an emotional distress case. See Total Carlot of the control of the control

band raised questions of fact whether his estranged wife and a private investigator violated his privacy under the Texas Constitution by secretly videotaping him in the bedroom of his home). The *Clayton* court held that, when a person goes into his or her bedroom, he or she generally has a legitimate expectation of privacy in his or her seclusion. *Id.* at 155. In more debatable contexts, the court suggested that factors to be considered in deciding an intrusion case include the private nature of the thing or place intruded upon and whether the defendant's conduct would be highly offensive and objectionable to a reasonable person. *Id.* at 152.

^{262.} See Cramer, 209 F.3d at 1133 (commenting that claims for emotional and negligent infliction of emotional distress "are 'parasite' claims that track the principal claim for invasion of privacy").

^{263.} Salazar, 2000 U.S. Dist. LEXIS at **18-19.

^{264.} Cramer, 209 F.3d at 1133.

^{265.} Id.

^{266.} Creel, 771 N.E.2d at 1282.

^{267.} See e.g. id. at 1283 (holding that secret videotaping of the plaintiff as she played piano for a congregation at an open church service "did not rise to the level of outrage necessary to support a claim for intentional infliction of emotional distress").

2003] CCTV and Other Video Security Technology

D. A Comparative Look at the United Kingdom: Informing the United States' Perspective of CCTV

No country utilizes CCTV more than Great Britain.²⁶⁸ While there is not an exact count, it is estimated that there are at least two and one-half million cameras in the country, with more being added daily.²⁶⁹ From the city of London, where a person is recorded a thousand times per day, to the rural areas of the country, cameras are found everywhere.²⁷⁰ With the prevalence of cameras as surveillance tools, issues dealing with privacy are addressed in statutes, codes of practice, and procedural manuals, which are all continuing to evolve to keep abreast of new technology and public concerns for privacy and the ethical use of technology.

While these concerns remain relevant, it may be said that, in general, public support for the technology is strong.²⁷¹ In contrast to the fundamental debate that characterizes the United States' experience to date, issues in the United Kingdom focus on the codes of practice and procedures to insure that they are fluid and reflect judicial decisions within the United Kingdom and the European Union.²⁷² The model emphasizes the affirmative effort to define appropriate limitations on governmental use of such systems.

^{268.} Burrows, supra n. 4, at 1101.

^{269.} Michael J. Sniffen, *Big Brother to See All, Everywhere* (July 1, 2003) (available at http://www.cbsnews.com/stories/2003/07/01/tech/main561302.shtml).

^{270.} See Jason Ditton, Crime and the City: Public Attitudes towards Open-Street CCTV in Glasgow, 40 British J. Criminology 692, 692 (2000) (discussing how cameras can be found in shops, buses, car parks, small businesses, and the London underground).

^{271.} See e.g. id. at 693 (revealing in a survey that, "overall, there is a majority support for open-street CCTV in Glasgow").

^{272.} See generally infra nn. 283-434 and accompanying text (discussing Great Britain's laws, policies, and procedures concerning personal privacy).

1. CCTV in City Centers

The Home Office, ²⁷³ the Scotland Office, ²⁷⁴ and the Northern Ireland Office ²⁷⁵ have long received financial support for the use of CCTV in city centers as a means of reducing crime. ²⁷⁶ In fact, large sums of money ²⁷⁷ began to flow toward this effort in the mid-1990s and, in 2001, the Home Office distributed nearly eighty million pounds sterling (GBP) for such schemes in that year alone. ²⁷⁸ Governmental support of CCTV systems has focused upon their perceived ability to offer "potential beneficial effects on crime, fear of crime and increased public confidence." ²⁷⁹ It is this belief in crime prevention and public safety that must be weighed against the loss of liberty (privacy) brought about by the use of CCTV technology.

It is noteworthy, in the evaluation of this subject, that Great Britain does not operate under a constitutional model per se; rather, a set of common and statutory laws provide the framework of permissible governmental action.²⁸⁰ This framework has grown steadily, year-by-year, from about 1,200 new measures annually in the mid-1970s to approximately fifteen new laws being added by Parliament each day.²⁸¹ Added to those numbers are di-

^{273.} The Home Office—the government department responsible for internal affairs in England and Wales—works to ensure the protection and security of the public. Home Office, *Welcome to the Home Office*, http://www.homeoffice.gov.uk/default.asp (accessed Sept. 29, 2003).

^{274.} The role of the Scotland Office, a government department, is "to represent Scottish interests in matters . . . reserved to the United Kingdom Parliament and [to] promote the devolution settlement for Scotland." The Scottish Parliament, Scotland Office, http://www.scottishsecretary.gov.uk/what.htm (accessed Sept. 29, 2003).

^{275. &}quot;The role of the Northern Ireland Office is to support the Secretary of State for Northern Ireland in securing a lasting peace . . . in which a safe, stable, just, open and tolerant society can thrive and prosper." Northern Ireland Office, *About the NIO*, http://www.nio.gov.uk/about.htm (accessed Sept. 29, 2003).

^{276.} David Mackay, Self Interest: The True Reasons for Supporting Town Centre Systems: A Case Study 1 (unpublished MSc thesis, Scarman Ctr. U. of Leicester 2002) (copy on file with the Stetson Law Review).

^{277.} From 1994 until 1997, 205 million pounds sterling was awarded to city centers for the purchase of hardware and the initiation of CCTV schemes. *Id*.

^{278.} Home Office Crime Reduction Program Unit 2001, CCTV Initiative: Round 2 Successful Bids, http://www.crimereduction.gov.uk/cctv21 (accessed May 5, 2003).

^{279.} Mackay, supra n. 276, at 1.

^{280.} See B.M. Selway, *The Constitution of the UK: A Long Distance Perspective*, Com. L. World Rev. 2, 2–3 (2001) (explaining that the United Kingdom "is a unified state with an unwritten constitution").

^{281.} The United Kingdom Parliament, Protection of Freedoms: Remarks to the United Kingdom Parliament, http://www.publications.parliament.uk/pa/cm200203; select

rectives coming from the European Union, which require member nations to address issues of concern, like privacy, by passing laws leading to the uniform treatment of major human rights issues across all member states.²⁸²

2. Role of the European Union

Each member state of the European Union must incorporate the tenets of the European Convention on Human Rights into its laws.²⁸³ Great Britain has made great strides in accomplishing this directive in areas dealing with the protection of personal data, access to data, and general concepts of privacy. Dating back to the 1981 Council of Europe Convention on Personal Data Protection, member states ratified ideas of information sharing.²⁸⁴ Problems soon arose because of the difficulty multi-national companies had when they wanted to share employee information across national borders.²⁸⁵ As a result, Directive 95/46/EC was issued, requiring member states to address, within their own legal structure, procedures related to the legal basis for collecting data; rules of fairness for those collecting the data; and rights of those whose personal data is the subject of such collections. 286 Of specific importance for the pursuit of privacy rights, subjects of data should have a right to access the data collected, know with whom and where the data collected originated, and be able to correct any inaccurate data compiled.287

England complied with this Directive, passing the Data Protection Act of 1998²⁸⁸ and the Data Protection (Processing of Sen-

cm030225; select debtext; select 30225-10.htm (accessed Apr. 13, 2003).

^{282.} See e.g. European Commn. Press Release, European Commission Adopts Directive on Protection of Personal Data: Council Definitively Adopts Directive on Protection of Personal Data (July 25, 1995) (available at http://www.ieee-security.org/Cipher/ConfReports/ECprivdirective.html) (discussing a directive regarding protection of personal data).

^{283.} The European Conv. on Human Rights, art. I (1951). The European Convention on Human Rights was drafted in 1949 and ratified in 1951. Helen Fenwick, *Civil Liberties and Human Rights* 17, 118 n. 160 (3d ed., Cavendish Publg. Ltd. 2002). The United Kingdom signed it, but it did not become a part of British domestic law. *Id.* at 117. In 1966, British citizens were given the right to go to the European Court. *Id.* at 118.

^{284.} European Commn. Press Release, supra n. 282.

^{285.} Id.

^{286.} Id.

^{287.} Neil McIntosh, *UK Pushes Boundaries of Citizen Surveillance*, The Guardian (June 12, 2002) (available at http://www.guardian.co.uk/netprivacy/article/ 0,2763,736011,00. html).

^{288.} Data Protection Act, 1998, c. 29 (Eng.) (available at http://www.legislation.hmso.

sitive Personal Data) Order 2000.²⁸⁹ The Data Protection Act of 1998 articulates clear principles of data protection, as well as the rights afforded to data subjects,²⁹⁰ data that is considered exempt,²⁹¹ and enforcement and remedies for violations.²⁹² The Data Protection (Processing of Sensitive Personal Data) Order 2000, effective March 1, 2000, clarifies certain portions of the Data Protection Act of 1998 and articulates the circumstances leading to the processing of personal data of a sensitive nature.²⁹³ Further, these pieces of legislation specify the role of Data Controllers, the Data Commissioner, and others responsible for the fair and just protection of personal data.²⁹⁴

In another example, the Human Rights Act of 1998,²⁹⁵ the United Kingdom incorporated the European Convention on Human Rights into its law. Of special significance relating to privacy in general, and CCTV surveillance by public authorities specifically, are sections 6.1–6.6 and 7.1–7.11 of the Act. Within these sections, local authorities, or those responsible for implementing and maintaining CCTV, are prohibited from acting in any way contrary to the European Convention on Human Rights.²⁹⁶ Thus, a local government anywhere in the United Kingdom that employs CCTV as a public safety and/or crime reduction tool must abide

gov.uk/acts/acts1998/; select 19980029.htm).

^{289.} Data Protection (Processing of Sensitive Personal Data) Order 2000, (2000) SI 2000/417 (available at http://www.legislation.hmso.gov.uk/si/si2000/; select 20000417.htm).

^{290. 1998,} c. 29 at §§ 7–15.

^{291.} Id. at §§ 27-39.

^{292.} *Id.* at §§ 40–50.

^{293.} SI 2000/417 at art. 2, §§ 1-6.

^{294.} Data Protection Act, c. 29 at §§ 40–45; Data Protection (Processing of Sensitive Personal Data) Order 2000, SI 2000/417 at art. 2, §§ 1–10.

^{295.} Human Rights Act, 1998, c. 42 (Eng.) (available at http://www.legislation.hmso.gov.uk/acts1998/; select 19980042.htm). Royal assent occurred in November 1998, and the Human Rights Act came into full force in October 2000. Press for Change, Jack Straw Announces Implementation Date for the Human Rights Act, http://www.pfc.org.uk/news/1999/ho-hra.htm (accessed Sept. 23, 2003). Article Eight, Section One of the Human Rights Act of 1998 states that "[e]veryone has the right to respect for his private and family life, his home and his correspondence." c. 42 at art. 8, § 1. Article Eight, Section Two states that

[[]t]here shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Id. at art. $8, \S 2$.

^{296.} Id. at §§ 6.1–6.6, 7.1–7.11.

by European rules governing the privacy of citizens within the context of human rights.

3. Criticisms about Lack of Privacy

Even with the incorporation of human rights and general privacy concerns into British law, critics argue that "Britain has one of the worst records in the developed world for protecting the privacy of its citizens." Privacy groups are concerned that, in the wake of the terrorist acts of September 11, 2001, many countries, especially the United Kingdom, have, by their increased reliance on video surveillance, limited important aspects of the right to assemble, free speech protections, and, more specifically, privacy protections relating to phone and electronic records being obtained without a warrant. These same critics argue that the Data Protection Act of 1998 can do little, if anything, to protect citizens from the increasing use of video as a law enforcement surveillance tool. The best that can be anticipated is for the Data Protection Act of 1998 to be fully implemented and for protections to be extended to the data collected via CCTV.

4. Legislative Response to Criticism

One clear avenue available to citizens to gain knowledge of and access to their personal data is the Freedom of Information Act of 2000.³⁰¹ This Act, which passed Parliament in November 2000, will not be fully implemented until January 2005.³⁰² However, in the interim, the position of Information Commissioner has been established to handle freedom of information and data

^{297.} Stuart Miller, *UK Singled Out for Criticism over Protection of Privacy*, The Guardian (Sept. 5, 2002) (available at http://www.guardian.co.uk/netprivacy/; *select* UK Singled Out for Criticism over Protection of Privacy (accessed Apr. 5, 2003).

^{298.} The Electronic Privacy Information Centre, in the United States, and Privacy International, in the United Kingdom, have both been very critical of British privacy policies. *Id.* at ¶ 2.

^{299.} See id. (discussing anti-terror legislation in Britain and noting that there has been "an almost universal shift in the balance towards more surveillance and less privacy since September 11").

^{300.} Id. at ¶ 9.

^{301.} Freedom of Information Act, 2000, c. 36 (Eng.) (available at http://www.legislation.hmso.gov.uk/acts/acts/2000; select 00036—a.htm).

^{302.} Information Commissioner, Lord Chancellor's Implementation Timetable: Dec. 2001, http://www.dataprotection.gov.uk/dpr.foi.nsf/; select Timetable (accessed June 19, 2003).

protection issues.³⁰³ The Act is significant for privacy reasons because it gives a general right to access all types of recorded information held by public authorities.³⁰⁴ Each public authority is charged with the task of identifying the type and form of information it collects and holds.³⁰⁵ When the Act is fully implemented in January 2005, all public authorities will have to handle individual citizen requests for personal data.³⁰⁶ This legislation extends rights currently held under the Data Protection Act of 1998 to information held in paper and computer files, including all types of information held, whether personal or nonpersonal in nature.³⁰⁷

Clearly, not every piece of data collected about citizens is available under the Freedom of Information Act. Among the twenty-three exemptions³⁰⁸ included within the Act are data related to national security,³⁰⁹ some law enforcement information,³¹⁰ and other types of data more commercial in nature.³¹¹ For example, law enforcement data that could hinder the prevention of crime, if made available, would be exempt as long as, on balance, the withholding of the information outweighs the value of disclosing it.³¹²

Thus, in an effort by the British government to address some of the privacy concerns of its citizens and the European community, a series of laws have been passed that attempt to deal with a host of issues. This legislation covers the type of personal data kept, the form in which the data is kept, personal access to that data, mechanisms for the review of personal data, and procedures to handle perceived violations of existing laws. While the laws appear to be quite broad in scope, addressing privacy in areas

^{303.} Freedom of Information Act, c. 36 at § 47.

^{304.} *Id.* at § 1. In this case, public authorities would include, but not be limited to, schools, colleges, universities, hospitals, police, Parliament, doctors, dentists, pharmacists, and parole board.

^{305.} Id.

^{306.} Id.

^{307.} Id. at § 68.

^{308.} *Id.* at §§ 21–44.

^{309.} Id. at §§ 23, 24.

^{310.} Id. at § 31.

^{311.} Id. at § 43.

^{312.} Id. at § 44.

^{313.} Freedom of Information Act, c. 36; Data Protection Act, c. 29; Data Protection (Processing of Sensitive Personal Data) Order 2000, SI 2000/417.

2003]

CCTV and Other Video Security Technology

ranging from hospitals to housing, further attention is necessary to explore the intersection of privacy and law enforcement.

5. Privacy and the Police

Rules governing the actions of law enforcement personnel can be found in a variety of Acts,³¹⁴ including the Protection from Harassment Act of 1997,³¹⁵ the Interception of Communications Act of 1985,³¹⁶ the Intelligence Services Act of 1994,³¹⁷ and the Local Government Act of 2000.³¹⁸ However, the focus of a commentary on CCTV and privacy naturally emphasizes legislation where primary attention is on the role of police in the United Kingdom.

In 1984, Parliament passed the Police and Criminal Evidence Act, ³¹⁹ also known as PACE. This law clarified and updated earlier legislation. ³²⁰ Relevant sections of PACE deal with the ability to arrest without warrants in cases where there are possible prison terms of five or more years. ³²¹ Arrests without warrants generally require necessity, ³²² and PACE articulates the rules governing these types of police encounters. ³²³ All that is required for an officer to arrest without a warrant is "reasonable grounds," as defined by general practice, to believe that the arrest is necessary. ³²⁴ Thus, potential exists for discriminatory application of the broad

^{314.} For the purposes of this Article, Acts dating from 1984 will be given primary focus. This cut-off date was chosen because that was the year of PACE, a very significant piece of legislation. *Infra* nn. 319–341 and accompanying text (discussing PACE).

 $^{315.\ 1997,\} c.\ 40\ (Eng.)$ (available at http://www.legislation.hmso.gov.uk/acts/acts1997; $select\ 1997040.htm).$

^{316. (1989)} SI 1989/489 (available at http://www.hmso.gov.uk/si/si1989/Uksi_19890489_en_1.htm).

^{317. 1994,} c. 13 (Eng.) (available at http://www.legislation.hmso.gov.uk/acts/acts1994/Ukpga_19940013_en_1.htm).

^{318. 2000,} c. 22 (Eng.) (available at http://www.hmso.gov.uk/acts/acts/2000/20000022.htm).

^{319. (1988)} SI 1988/1200 (available at http://www.hmso.gov.uk/si/si1988/Uksi_198811200_en_1.htm).

^{320.} Magna Carta Plus, *Police and Criminal Evidence Act—1984: Summary*, http://www.magnacartaplus.org; *select* United Kingdom Acts of Parliament Pertinent to Civil Liberties, *select* Police and Criminal Evidence Act 1984—Summary (accessed Apr. 3, 2003) [hereinafter *PACE Summary*].

^{321.} Id.

^{322.} *Id.* "Necessity" includes failure to identify oneself when asked by law enforcement, a clear likelihood that a person would fail to appear in court when ordered, and the potential for continued criminal behavior if police do not take the person into custody. *Id.*

^{323.} Id.

^{324.} Id.

concept of "reasonable grounds" to groups like the homeless.³²⁵ In an illustrative case, police arrested a person riding a bicycle after he refused to put his hands on the handlebars and give his name and address to the police.³²⁶ The case was affirmed on appeal,³²⁷ indicating that an individual has no right to privacy when police officers ask specific, identifying questions.

PACE was extended to incorporate Codes of Practice under Order 1988, 328 Order 1990, 329 and finally, Order 1995, 330 which vacated the two previous Codes of Practice.331 Under Order 1995, clear rules for the maintenance of privacy, among other procedures like detention, seizure of property, and suspect treatment by the police, 332 were specified in the areas of powers of stop and search, searches of premises, identification of persons by police, and tape-recording of police interviews. 333 The new rules became effective April 10, 1995, 334 and clearly fall on the side of expanded powers for police, with decreased privacy for citizens. For example, the police now have the right to hold citizens for up to ninetysix hours without bringing charges. 335 Additionally, the police possess the ability to arrest without a warrant when citizens refuse to give their proper names and/or addresses, 336 and, for all practical purposes, any privacy associated with the right to remain silent no longer exists.

Further, Order 2001 under PACE³³⁷ requires tape-recording of all interviews conducted by police at police stations.³³⁸ Order

^{325.} Id.

^{326.} Id.

^{327.} Id.

 $^{328.\ (1988)\} SI\ 1988/1200$ (available at http://www.legislation.hmso.gov.uk/si/si1988/Uksi_19881200_en_1.htm).

 $^{329.\ (1990)}$ SI 1990/2580 (available at http://www.legislation.hmso.gov.uk/si/si1990/; select Uksi 19902580).

 $^{330.\ (1995)}$ SI 1995/450 (available at http://www.legislation.hmso.gov.uk/si/si1995/; select Uksi 19950450).

^{331.} Id.

^{332.} Id. at § 1(a)-(e).

^{333.} Id.

^{334.} Id. at § 3.

^{335.} Id. at § 3(1), 3(3).

^{336.} PACE Summary, supra n. 320. Silence can be an inference of guilt upon questioning by police. Id. In many instances, any exculpatory information, such as an alibi that is not offered to police when asked, is often lost forever and cannot be used in later court proceedings.

^{337. (2001)} SI 2001/2480 (available at http://www.hmso.gov.uk/si/si2001/20012480.htm).

2003]

353

CCTV and Other Video Security Technology

2002³³⁹ under the same 1984 Act also requires visual recording of interviews in twelve specific police authorities throughout the United Kingdom.³⁴⁰ These rules requiring taping (either audio or video) suggest that, as in the United States, little privacy exists once a person is at the police station.³⁴¹

In an effort to control law enforcement and government entities' access to personal information, the European Parliament issued Directive 97/66/EC. This Directive required member states to pass initiatives to deal with the confidentiality of communications, to institute controls on the interception of private conversations, and to control surveillance activities. As a result, the Regulation of Investigatory Powers Bill was passed. The thrust of this bill addresses growing concerns voiced by the Data Protection Commissioner and others with regard to a number of privacy issues, including, for example, the lack of external oversight regarding warrants for the interception of data by law enforcement, issues related to law enforcement access to protected

^{338.} Id.

 $^{339.~(2002)~{\}rm SI}~2002/1069~{\rm (available}~{\rm at}~{\rm http://www.hmso.gov.uk/si/si2002/20021069.htm)}.$

^{340.} *Id.* at §§ 2–3.

^{341.} See Ahmad v. Superior Court, 215 Cal. App. Supp. 3d 528, 534–536 (Cal. Super. App. Dept. 1989) (bound with Cal. App. 3d) (regarding police interception of conversation between a suspect and his mother in a police interrogation room); Belmer v. Cmmw., 553 S.E.2d 123, 128 (Va. App. 2001) (observing that "the federal courts continue to find a suspect has no reasonable expectation of privacy in areas controlled by the police"). An exception to the rule may exist where the police "lull" a suspect into believing that his or her conversation will be private. Id. at 129 (citing People v. A.W., 982 P.2d 842, 848–849 (Colo. 1999)); cf. Lanza v. N.Y., 370 U.S. 139, 141 (1962) (electronic interception of prisoner's conversation with his brother); U.S. v. Hearst, 563 F.2d 1331, 1344–1346 (9th Cir. 1977) (regarding prisoner's conversation with a visitor).

^{342.} European Parliament, Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector, http://europa.eu.int/ISPO/infosoc/ telecompolicy/en/harmony.htm; select Directive97/66/EC (accessed Apr. 3, 2003).

^{343.} *Id*. at art. 5.

^{344.} The United Kingdom Parliament, Regulation of Investigatory Powers Bill, http://www.parliament.the-stationery-office.co.uk/pa/ld199900/ldbills; select 061; select 2000061.htm (accessed June 15, 2003).

^{345.} Information Commissioner, Response of the Data Protection Commissioner to the Government's Regulations of Investigatory Powers Bill: A Briefing for Parliamentarians, http://www.dataprotection.gov.uk/dpr/dpdoc.nsf; select Codes of Practice Our Responses & Other Papers, select Regulation of Investigatory Powers (accessed Apr. 13, 2003).

^{346.} *Id.* at Introduction § 2.

electronic information, 347 and the lack of warrants required for access to communications data. 348

Concerns dealing with lack of external oversight where interception warrants are concerned can be handled differently, based upon the purpose of the interception. When national security is at stake, administrative warrants can be applied. In contrast, in cases dealing with crime detection and prevention, judicial warrants are more appropriate. Here, judicial oversight should be at the point of issue of the warrant and also during any criminal proceedings that result from evidence gathered as a result of the interception.

Further, the Regulation of Investigatory Powers Act (RIPA)³⁵³ provides for judicial scrutiny of all cases involving surveillance of an intrusive nature.³⁵⁴ The privacy protection applies to the covert surveillance of residential areas, private vehicles, or any location where the citizen has a legitimate expectation of privacy, such as a doctor's office or pharmacy.³⁵⁵ RIPA goes further to establish criminal sanctions when proper authorization is not secured prior to the onset of the surveillance.³⁵⁶

The applied reality of RIPA may be quite different. Since its passage in February 2000, critics have noted that non-law-enforcement officials³⁵⁷ can use the law under the vague "national security" or "any purpose" provisions designated by the Home Secretary clause.³⁵⁸ The law was originally designed as a law enforcement tool to root out criminal gangs and networks, while si-

```
347. Id.
```

^{348.} Id.

^{349.} See generally id. at §§ 4–7 (addressing external scrutiny of warrants).

^{350.} Id. at § 7.

^{351.} Id.

^{352.} Id. at § 4.

 $^{353.\ 2000,}$ c. 23 (Eng.) (available at http://www.hmso.gov.uk/acts/acts2000/20000023.htm).

^{354.} *Id*.

^{355.} *Id*.

^{356.} *Id.* (creating the offense of unlawful interception of communications in Clause One; however, there are no specific penalties identified therein).

^{357.} David Leigh & Richard Norton-Taylor, *Is Anybody Listening? Why Have Patricia Hewitt and Harriet Harman Abandoned Civil Liberties?* The Guardian (June 12, 2002) (available at http://www.guardian.co.uk/comment/story/o,3604,735848,00.html). The trade secretary and the solicitor general are examples of non-law-enforcement officials taking advantage of the Act's vague terminology. *Id*.

^{358.} *Id*.

multaneously protecting the privacy of the average citizen; however, it has been transformed into a vehicle used by non-law-enforcement entities to monitor community groups, journalists, and other critics of governmental agencies. For example, agencies like the Office of Fair Trading and the Food Standards Agency can use the law's covert surveillance properties to access pagers, e-mails, mobile phone records, cars, and homes. RIPA prevents persons who are targeted by intrusive surveillance from appealing under the Human Rights Act, and they are only allowed review by a tribunal that meets in secret.

Since the passage of RIPA, British police have been able to access, without judicial oversight, communication logs and general surveillance of communications by citing national security concerns.³⁶² To prevent public knowledge of some of the surveil-

^{359.} Id.

^{360.} Id.

^{361.} Id.

^{362.} Stuart Millar & Richard Norton-Taylor, Police in New Email Spying Row: Secret Plan to Prevent Disclosure at Trials, The Guardian (June 18, 2002) (available at http://www.guardian.co.uk/netprivacy/article/0,2763,739360,00.html). In the wake of September 11th, laws such as RIPA and the USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001), focus attention on terrorist activities. The USA PATRIOT Act expands wiretapping under the Foreign Intelligence Surveillance Act of 1978, by, inter alia, authorizing "roving" wiretaps; permitting a single court order to authorize the use of "pen registers" and "trap and trace" devices modifying search warrant guidelines in cases of suspected terrorism; broadening the basis for obtaining a warrant to conduct electronic surveillance of telephones, e-mail, or premises by requiring only that foreign intelligence is "a significant purpose" (rather than the "primary purpose") of the surveillance, with no required showing of probable cause to suspect criminal activity; and permitting police to rely on the consent of employers, school authorities, and libraries to monitor an individual's e-mail or Internet browsing without a warrant. Michael T. McCarthy, Student Author, USA PATRIOT Act, 39 Harv. J. on Legis. 435, 444-446 (2002); Robert Ellis Smith, The Impact of the Federal Anti-Terrorism Legislation upon Government Surveillance and Ordinary Americans, 50 R.I. B.J. 11 (Mar./Apr. 2002). Additionally, the United Kingdom has applied pressure on the European Parliament to encourage internet service providers and phone companies to maintain customer logs for an unspecified period of time. The information requested would amount to the collection of a roadmap of each person contacted, using e-mail and Web sites visited, resulting in a complete picture of an individual's travels in cyberspace. Caspar Bowden, CCTV for inside Your Head: Blanket Traffic Data Retention and the Emergency Anti-Terrorism Legislation, 2002 Computer & Telecomm. L. Rev. 20, 21 (2002). RIPA spells out the provisions for such data collection, including regulations governing the collection. Id. at 22. The United Kingdom Anti-Terrorism Crime and Security Bill (ATCS), Part 11, Retention of Communications Data, will lend further support to RIPA, as it applies to collecting cyber information on citizens. Id. at 21. ATCS uses broad terminology to allow for traffic analysis and allows for the capture of information about who citizens talk to (by phone and e-mail), where citizens physically go (by tracking mobile phones), and what citizens read online (by logging the Web addresses visited). Id. ATCS will also mandate that internet and phone company records be held in

lance techniques employed by law enforcement, public interest immunity certificates have been sought as a means of preventing specific disclosures at trial.³⁶³ Public interest immunity certificates are designed to make relevant material available to all parties while maintaining the confidentiality of documents when disclosure of their contents would be damaging to the government or an agency.³⁶⁴ The use of public interest immunity certificates may be viewed as an inappropriate balance—one where law enforcement's ability to access communications outweighs the rights of citizens to maintain privacy. Additionally, the abuses of the powers available under RIPA may usurp the fundamental right to a fair trial.

The Criminal Justice and Public Order Act of 1994³⁶⁵ also deals with obtaining computer-held information.³⁶⁶ Additionally, it authorizes local governments to provide, maintain, and operate CCTV systems and to provide telecommunications systems—which may be run without a license—for the purposes of integrating these systems.³⁶⁷ Local governments are vested with the power to provide the apparatus for CCTV and to collect information resulting from the implementation of their CCTV systems.³⁶⁸ The seminal case considering the legitimacy of the establishment of systems and the limited judicial oversight, which protects against their abuse, is the *Case of Peck v. The United Kingdom*.³⁶⁹ Geof-

what amounts to a "traffic data warehouse" for exclusive use by police and security agencies. *Id.* A police official can authorize collection of the data without a judicial warrant. *Id.* The United Kingdom has urged the European community to follow suit and mandate similar regulations for internet providers on the continent. Government agencies could certainly interpret such provisions of anti-terrorism legislation to permit the expanded use of CCTV and other video technology.

363. See Miller & Norton-Taylor, supra n. 362 (discussing public interest immunity certificates).

364. See Regina v. Gov. of Brixton Prison, [1990] 1 W.L.R. 281, 286 (denying access to requested documents based upon the potential damage to the governments involved if the documents were made public). The defendant filed a habeas corpus action challenging extradition to Hong Kong on charges of conspiracy, bribery, and theft. Id. at 281. The defendant requested access to documents relating to communications between the Home Office and the government of Hong Kong. Id.

365. 1994, c. 33 (Eng.) (available at http://www.hmso.gov.uk/acts/acts1994/; select Ukpga19940033en1.htm).

366. Id.

367. Id . Sections 161, 162, and 163 deal with closed-circuit television operated by local authorities and access to computer-held information. Id .

368. Id.

369. No. 44647/98, Eur. Ct. H.R. (2003) (available at http://www.echr.coe.int/Eng/Judgments.htm; select Search the Caselaw—Hudoc, enter application no. 00044647/98,

2003]

CCTV and Other Video Security Technology

frey Dennis Peck, a British citizen, brought the case, by application, "against the United Kingdom of Great Britain and Northern Ireland lodged with the European Commission of Human Rights . . . under former Article 25 of the Convention for the Protection of Human Rights and Fundamental Freedoms." Peck complained about the disclosure of CCTV footage to the media, which resulted in images of himself being published and broadcast widely on television and in the print press. He alleged that the disclosure should be held to violate his rights under Articles Eight and Thirteen of the Convention. The strength of the Convention.

In February 1994, the Brentwood Borough Council approved guidelines for both the operation and management of a CCTV system, under the authority of Section 163 of The Criminal Justice and Public Order Act of 1994. 373 The system provided the Council's monitoring operator with a direct visual and audio link to the police, and images being captured could be switched through to the police in the operator's discretion.³⁷⁴ Peck, suffering from depression, cut his wrists with a kitchen knife in an apparent suicide attempt as he walked alone towards a central junction in the center of Brentwood. 375 A CCTV camera, mounted on the traffic island in front of the junction, filmed his movements, and the system operator alerted police, who rendered medical assistance and then brought Peck to the police station, where they detained him under the Mental Health Act of 1983. The Council subsequently permitted the release of "regular press features" about its CCTV system.377 The first feature, as well as several later features in newspapers and on television, included both unmasked and partly, but ineffectively masked, photographs of Peck and descriptions of the incident used to illustrate the effectiveness of CCTV.378 When

select Case of Peck v. The United Kingdom).

^{370.} Id. at § 1.

^{371.} *Id.* at § 52.

^{372.} Id. at §§ 52, 91.

^{373.} Id. at §§ 9, 29.

^{374.} Id. at § 9.

^{375.} Id. at § 10.

^{376.} Id. at §§ 10, 11.

^{377.} Id. at § 12.

^{378.} Id. at §§ 13–21. Two still photographs were released in CCTV News on October 9, 1995, and Peck's face was not masked. Id. at § 13. On October 12, 1995, the Brentwood Weekly News ran a still picture on the front page, and again, Peck's face was not masked. Id. at § 14. On October 13, 1995, the Yellow Advertiser ran an article with a photograph of

Peck learned he had been filmed on CCTV and was an identifiable subject of these features, he pursued administrative remedies before the Broadcast Standards Commission and the Independent Television Commission, and ultimately sought judicial review.³⁷⁹

The High Court rejected his application, finding that the legitimate governmental "purpose of section 163 of the Criminal Justice and Public Order Act 1994... was to empower a local authority to provide CCTV equipment in order to promote the prevention of crime or the welfare of victims of crime," and concluding "that the Council had the power to distribute the CCTV footage to the media by virtue of section 111 of the Local Government Act 1972 in the discharge of their functions under Section 163 of the 1994 Act." The High Court did, however, note that the incorporation of the European Convention on Human Rights into British law might provide a future right of privacy, prohibiting the acts at issue. Beck then petitioned the European Court of Human Rights.

The European Court of Human Rights recognized the statutory authorization and regulation of surveillance under the Interception of Communications Act of 1985, the Intelligence Services Act of 1994, and the Police Act of 1997. It also noted that "[t]he purpose of the Regulation of Investigatory Powers Act [of] 2000 is to ensure that the relevant investigatory powers of the authorities are used in accordance with human rights" and that many users of CCTV must comply with the provisions of the Data Protection Act of 1998. Turning to Peck's allegation of rights under Article Eight of the Convention, the Court recognized the existence of "a

Peck taken from the CCTV footage. *Id.* at § 15. On October 17, 1995, Anglia Television ran the footage with Peck's face masked, although his facial hair and hairstyle were distinctive, permitting his identification by those who knew him. *Id.* at § 16. On February 16, 1996, the *Yellow Advertiser* ran a second article with the same photograph, resulting in many people recognizing Peck. *Id.* at § 19. On March 9, 1996, he was shown on ads for a *Crime Beat* episode. *Id.* at § 21.

^{379.} Id. at §§ 24–28.

^{380.} *Id.* at §§ 29, 30. The Criminal Justice and Public Order Act of 1994, Section 163 (effective Feb. 3, 1995) provides, inter alia, that a local authority may promote the prevention of crime or the welfare of the victims of crime by providing for the installation and operation of a CCTV system, which is exempted from the license requirements of the Telecommunications Act of 1984. *Id.* at § 29.

^{381.} Id. at § 32.

^{382.} Id. at § 1.

^{383.} Id. at § 46.

 $^{384. \} Id.$

zone of interaction of a person with others," outside the home or other private premises, "which may fall within the scope of 'private life." Describing this zone of privacy, and citing prior authority, the Court observed that a person who walks down the street, subject to observation by any other member of the public, may be subject to monitoring by a CCTV system without implicating his or her expectation of privacy. However, the recording and the use of the data obtained may raise concerns for privacy. 387

Noting that Peck had no objection to the CCTV monitoring of his movements *per se*, the Court focused on the issue of the disclosure of his identifiable image and commentary to the public.³⁸⁸ Finding that Peck was not on the street for the purpose of participating in any public event, the Court held that he could not have foreseen the extent to which his actions would have been seen publicly.³⁸⁹ The Court concluded that "the disclosure by the Courcil of the relevant footage constituted a serious interference with the applicant's right to respect for his private life."³⁹⁰

The Court held, however, that such an intrusion might be legally justified by the local authority's use of CCTV to prevent crime and promote the welfare of victims of crime, noting with approval the Council's authority to distribute CCTV images to the media, pursuant to Section 111 (1) of the Local Government Act of 1972, in the discharge of its functions under Section 163 of the Criminal Justice and Public Order Act of 1994.³⁹¹ However, the legitimate governmental determination of the parameters of public interest and competing interests in privacy is dependent, among other things, upon "the nature and seriousness of the interests at stake and the gravity of the interference."³⁹²

Applying these principles, the Court held that, when the instant case did not involve disclosure of footage of the commission of a crime, and when the Council could have identified Peck through inquiries with the police, thereby obtaining Peck's con-

^{385.} *Id.* at § 57 (quoting *P.G.* & *J.H.* v. The United Kingdom, no. 44787/98, Eur. Ct. H.R., § 56 (2001)).

^{386.} Id. at § 58 (quoting P.G. & J.H., no. 44787/98 at § 57).

^{387.} *Id.* at § 59.

^{388.} Id. at § 60.

^{389.} Id. at § 62.

^{390.} Id. at § 63.

^{391.} Id. at §§ 66, 67.

^{392.} Id. at § 77.

sent prior to disclosure, its disclosure of the CCTV material to the public, through both print and television media, intruded upon protections of private life in violation of Article Eight of the Convention.³⁹³

The significance of this finding clearly relates to the purpose of CCTV in general, and, specifically, the release of CCTV footage to the media. The result of this case for CCTV users in the United Kingdom is that,

very few images have been shown for entertainment purposes on television since the filing of the *Peck* case, because standards exist to govern their release. It is the existence of these standards that has led to the responsible use of CCTV and continuing public support.³⁹⁴

6. Regulations Governing Procedures and Practice of CCTV

After many years of experience using CCTV in the United Kingdom,³⁹⁵ by the mid-1990s there were organizations to represent the manufacturers but no counterpart for the end-users of the systems.³⁹⁶ It became apparent that a group composed of the actual users would be an asset for sharing information about technology, practice, regulations, and so forth. In 1996, the CCTV Users Group was established to represent end-users working in the United Kingdom.³⁹⁷

Soon after the organization of the CCTV Users Group, a twoyear process began to develop a Model Procedural Manual and a Model Code of Practice for end-users.³⁹⁸ The documents are based upon the belief that "everyone has the right to respect for his or her private life and family life and their home."³⁹⁹ Further, in addition to the clear concern about individual privacy, the group believes that no government should interfere with that right

^{393.} Id. at §§ 79-87.

^{394.} Peter Fry, Unmasked Footage Is Breach of Privacy Right: European Court, CCTV Today 4 (Mar./Apr. 2003).

^{395.} The use of CCTV by retailers began in earnest in 1967 and in town centers in 1985. CCTV User Group, *Model Code of Practice & Procedural Manual*, http://www.cctvusergroup.com/code_ofpr_ac_tice.htm (accessed June 12, 2003) [hereinafter *Procedural Manual*].

^{396.} Id.

^{397.} Telephone Interview with Peter Fry, Dir., CCTV Users Group (May 29, 2003).

^{398.} Procedural Manual, supra n. 395.

^{399.} Telephone Interview, supra n. 397.

unless national security, crime prevention, economic security of the country, or protection of the rights of all citizens is at stake. 400 Since no legislation specifically addressed the codes of practice or the procedures that should be invoked to guarantee these rights, the Standards Committee of the CCTV Users Group set about creating models that local authorities could use to insure the rights of privacy discussed above. 401 Once the model documents were finished, close contact was maintained with the British Home Office. 402

From its beginning in 1996, the CCTV Users Group has grown to include over 400 different organizations, involving nearly 600 individuals. The group publishes a journal, encourages system evaluation, and sponsors a YAHOO! e-mail discussion forum offering a help desk, all geared toward setting standards for the industry and for getting the most from current systems. The Model Code of Practice is used by over 200 public CCTV schemes in the United Kingdom. The Code of Practice includes (1) system objectives, (2) statements of purpose and principles, (3) provisions governing privacy and data protection, (4) accountability and public information, (5) system evaluation, (6) human resource issues, (7) control and opera-

^{400.} Id.

^{401.} CCTV User Group, Model Procedural Manual in Respect of the Operation of Closed Circuit Television: Setting Standards for the Industry i (internal publication of the CCTV User Group 1999) (copy on file with the Stetson Law Review) [hereinafter Model Procedural Manual].

^{402.} For example, the CCTV User Group has semi-annual conferences attended by Home Office representatives from both research areas and policy positions.

^{403.} CCTV User Group, CCTV User Group Constitution & Administrative Protocols, http://www.cctvusergroup.com; select Constitution and Protocols (accessed June 22, 2003). Included among these organizations are public area CCTV systems, local authorities, police forces, universities, airports, shopping centers, and hospitals.

^{404.} CCTV User Group, What Services Does the CCTV User Group Provide for Its Members? http://www.cctvusergroup.com; select Member Services (accessed June 22, 2003).

^{405.} CCTV User Group, Model Code of Practice for the Operation of Closed Circuit Television Based upon the CCTV User Group Model Documents (2001) (internal publication of the CCTV User Group 2001) (copy on file with the Stetson Law Review) [hereinafter Model Code of Practice].

^{406.} Telephone Interview, supra n. 397.

^{407.} Model Code of Practice, supra n. 405, at § 1.3.1.

^{408.} *Id.* at § 2.1, 2.1.1.

^{409.} Id. at § 3.

^{410.} Id. at § 4.

^{411.} Id. at § 5.

^{412.} Id. at § 6.

tion of cameras, 413 (8) access and security of monitoring rooms, 414 (9) management of recorded material, 415 and (10) video prints. 416

The Model Code of Practice offers a series of documents, in appendix form, that can be modified to fit the local needs of endusers. Included are forms that allow for the identification of key personnel and their specific responsibilities, 417 which may vary from one scheme to another; excerpts from the Data Protection Act of 1998 that specifically apply to CCTV users; 418 standards for the release of data to third parties; 419 declarations of confidentiality; 420 sample request forms for information held on the CCTV system; 421 and guiding principles of the Data Protection Act. 422 The thoroughness of the Model Code of Practice allows a new scheme to be aware of all governing issues related to the application of CCTV from its inception. While this is only a model, it is easily adapted to the individual needs of a given jurisdiction, based upon recommendations from local solicitors.

The Model Code of Practice sets the standards for the legal and ethical management of a CCTV scheme. The Model Procedural Manual, on the other hand, offers specific guidelines for the day-to-day operation of such a scheme. Included within the Model Procedural Manual are suggestions for the selection and screening of CCTV operators, rules governing the control and operation of cameras, access to and security of the monitoring room, management of recorded material, and record keeping, as well as a section on dealing with the media.

```
413. Id. at § 7.
```

^{414.} Id. at § 8.

^{415.} *Id.* at § 9.

^{416.} Id. at § 10.

^{417.} Id. at app. A.

^{418.} Id. at app. B.

^{419.} Id. at app. C.

^{420.} *Id.* at app. E. These are to be completed by the CCTV managers, declaring that they understand their duties and cannot disclose any information gained in connection with their CCTV system.

^{421.} Id. at app. G.

^{422.} Id. at app. I.

^{423.} Model Procedural Manual, supra n. 401.

^{424.} Id. at § 2.

^{425.} Id. at § 3.

^{426.} Id. at § 4.

^{427.} Id. at § 5.

^{428.} *Id.* at § 5(X)–5(XIII).

^{429.} Id. at § 9.

Model Code of Practice, the Model Procedural Manual offers, in appendix format, samples of emergency procedures, 430 witness statement forms, 431 and excerpts from laws of direct importance to the successful and legal completion of one's job as a CCTV manager or operator.432

The Model Code of Practice and Model Procedural Manual have been developed and modified to maintain concern for individual privacy while allowing CCTV the greatest flexibility as a crime fighting tool. 433 The efforts of the CCTV Users Group have not gone unnoticed by the Home Office. In their annual funding schemes, the Home Office strongly encourages local authorities seeking funding to adopt these documents and to adapt them to the individual needs of their schemes. To date, over 200 local authorities have done so. 434

7. Summary

In the United Kingdom, concerns about privacy and the operation of CCTV schemes are governed by a national effort to uphold the laws of the European Union and the United Kingdom. National information sharing via the CCTV Users Group and conferences allow local authorities to incorporate the latest laws and court decisions into their daily practice. Great care has been given to the construction and implementation of codes of practice and procedural manuals, thus leading to few legal challenges to the use of CCTV within public areas. While not a perfect system, the United Kingdom, with its long history of CCTV use, has made great strides to balance the privacy rights of its citizens against the legitimate security needs of the country and offers an informative comparative paradigm for the evaluation of statutory efforts and the establishment of practice and procedural protocols in the United States. While judicial guidance is minimal at this writing, the decision of the European Court of Human Rights in the *Peck* case permits some comparison of both the concept of privacy and the proper role of the courts in the oversight of legisla-

^{430.} Id. at app. J.

^{431.} Id. at app. C.

^{432.} *Id.* at app. B.

^{433.} Model Code of Practice, supra n. 405, at § 1.2; Model Procedural Manual, supra n. 401. at i.

^{434.} Telephone Interview, supra n. 397.

tive bodies, local governments, law enforcement agencies, and citizen action groups regarding the promulgation and administration of CCTV practices and procedures.

VI. CONCLUSION

The decision whether to use silent video surveillance technology in certain environments and situations, as well as decisions regarding the extent of its use, raise serious constitutional and tort law questions. The wide array of technology that is available and emerging certainly encourages the use of video security systems. However, the design and implementation of any such system, as well as its periodic enhancement, must recognize legal parameters that both limit and expand rights and responsibilities.

Many explicit and implied suggestions may be taken from our comments. However, a few suggestions rise above the others and are emphasized because of our concern that the pressure for more security and anti-terrorism measures will prevent the kind of discourse that should accompany developing law. Put simply, federal and state constitutional privacy protections must be explicitly extended to the covert use of video cameras and the "open" use of sensory-enhancing video technology. The difference of opinion within the Supreme Court about the extent to which the rule of *Kyllo* should address rapidly emerging video security technology must be resolved by the Court or Congress, and that resolution must revisit the Court's decisions in *Katz* and *Ortega* in the light of Judge Fabe's interpretation of those cases and other influential state court decisions cited in her dissent in Cowles. 435 The question of great public importance that must be answered is the question posed by Granholm and addressed in the line of federal and state court cases decided since her seminal work on the subject: Is there a zone of constitutionally protected privacy, even in public places, which must be protected against unreasonable intrusion by sensory-enhanced video technology?⁴³⁶

^{435.} See Taslitz, supra n. 15, at 145 (raising serious questions about Katz and emphasizing that the Court's opinion in Kyllo confined its protection to the home, ruling that "[s]ense-enhancing technology that reveals any information regarding the interior of the home constitutes a search . . . 'where . . . the technology in question is not in general public use"). Id.

^{436.} Granholm, supra n. 3.

2003] CCTV and Other Video Security Technology

Finally, there is a need for scientific research to evaluate measures that are being put in place. Emerging federal law appears to be overly influenced by broad-scale concerns for homeland security, which may obscure or even undermine a reasoned approach to a rule of law that establishes constitutionally reasonable parameters for the use of video security technology, and which subjects the use of such technology to preliminary scientific research evaluating its effectiveness as deployed to date. Simply put, the law must "catch-up" with technology, and a balance must be struck between security interests and privacy interests with direct reference to the "public" and covert use of video security technology.

Political leaders of both major national political parties in the United States have called for protective legislation, and such legislation appears necessary unless federal and state courts, in the absence of any statutes, can define appropriate constitutional limitations upon the use of the technology. Justice Stevens, writing for himself, the Chief Justice, and Justices O'Connor and Kennedy in Kyllo, argues for judicial restraint and against an "all-encompassing" constitutional rule, suggesting that legislators should deal with the emerging issues arising from the deployment of video security technology. 438 Perhaps the dissenters are correct, in the sense that federal and state legislatures are better prepared to conduct investigations and initiate research, which would support scientific factfinding, as a condition precedent to the enactment of definitive laws on the subject. However, it is beyond cavil that the courts have a role in resolving the constitutional question at the foundation of the balance between safety and security, and the rights of citizens in a democracy to demand a reasonable zone of privacy. 439

^{437.} Such research must be national in scope and must include pre-deployment projects that permit the scientifically legitimate assessment of the technology in the context of other variables affecting crime reduction.

^{438.} See Kyllo, 533 U.S. at 51 (Stevens, J., dissenting) (stating, "It would be far wiser to give legislators an unimpeded opportunity to grapple with these emerging issues rather than to shackle them with prematurely devised constitutional constraints").

^{439.} Solove observes that "the concern over privacy has escalated into an essential issue for freedom and democracy." Solove, *supra* n. 2, at 1089. Yet, despite the need to define the nature and scope of this important right, legal and social theorists remain challenged in evaluating traditional views of privacy and assessing new approaches.

On the policy side, evaluating video monitoring policy, staffing, training, and budget issues are essential, in both public and private contexts, and should demand a collaborative effort involving all elected bodies and policy administrators with responsibility for public safety and security. Issues of ethics and professionalism exist as well, and must dominate any protocol defining the implementation of such technology.⁴⁴⁰

The absence of much caselaw deprives us of the administrative efficiency we seek in the law, but the caselaw that does exist gives guidance, rich in common sense, as well as applicable constitutional and tort law principles that can be analogized with minimal intellectual uncertainty. The challenge is whether law enforcement administrators, government agencies, and employers are willing to devote serious research and planning, as well as budgeting (for training, staffing, maintenance, etc.) to this aspect of policing and security, and whether a shared commitment to the appropriate use of technology may be obtained through any sort of "voluntary" protocol. 441

This last facet of video surveillance planning is especially delicate. Citizens who appear to desire video surveillance in hotels, convenience stores, and parking lots seem willing to sue landowners and places of public accommodation, or employers for negligence when the risk of criminal assault is foreseeable and video surveillance is not employed. Yet some of these same citizens have a general concern about the use of such technology by police, fearing the risk of a "big brother" culture that violates notions of privacy, and by employers for similar reasons. These inherently conflicting interests must be openly identified, discussed, and balanced politically as well as legally.

The law seeks an appropriate paradigm, but successful law and policy approaches to the use of silent video by police, employ-

^{440.} In addition to the ABA's efforts to establish standards, voluntary associations of concerned security and law enforcement groups, such as the Private Sector Liaison Committee, have engaged in considerable and commendable efforts to define an appropriate ethical protocol governing the use of such technology by cities. However, in the absence of law, these groups lack the authority of courts and legislatures to protect constitutional privacy interests and cannot require the adoption of particular ethical protocols by cities or private sector entities employing sensory-enhancing technology.

^{441.} Professor Taslitz recalls and underscores Justice Harlan's observation in his dissenting opinion in *U.S. v. White*, 401 U.S. 745, 786 (1971), in which Justice Harlan stated that an individual's "sense of security" requires more protection than mere "self-restraint by law enforcement officials." Taslitz, *supra* n. 15, at 138.

2003] CCTV and Other Video Security Technology

ers, educational institutions, and commercial establishments must involve all interested parties—citizen groups, law enforcement and other public officials, employers, business leaders, civil rights lawyers, and personal injury lawyers—and their collaboration in the balancing of interests in safety, security, and crime reduction, with the enforceable protection of reasonable principles of privacy.