Harvard Journal of Law & Technology
Volume 10, Number 3 Summer 1997

TECHNOLOGICALLY-ASSISTED PHYSICAL SURVEILLANCE: THE AMERICAN BAR ASSOCIATION'S TENTATIVE DRAFT STANDARDS

Christopher Slobogin[*]

TABLE OF CONTENTS

---

* Professor of Law, Alumni Research Scholar and Associate Dean, University of Florida College of Law; Reporter, American Bar Association Task Force on Technology and Law Enforcement. More than is typically the case with a law review article, I owe a debt of gratitude to many others, most particularly the members of the Task Force, *see infra* note 6, who are largely responsible for the ideas described in this Article (although any errors in describing the deliberations of the Task Force are mine). For their special contributions to this effort, I thank Sheldon Krantz, Chair of the Task Force on Technology and Law Enforcement; Judy McBride, Director of the ABA's Criminal Justice Standards Committee during the Task Force's deliberations; Wayne LaFave, whose comments contributed significantly to the ideas expressed in this Article; and Christopher C. Look, my research assistant.

I. INTRODUCTION

It is the year 2001. The Chicago police know that a large and violent drug ring is operating out of Slumville, a downtown section of the city. The gang manufactures drugs, sells them on the streets, and distributes them to other locations in Chicago and outlying areas. Wary of electronic surveillance, the group never uses phones or pagers but instead conducts all of its transactions face-to-face. The city is fed up with having an illegal drug factory in its midst.

The new chief of police decides to mount an aggressive effort to close down the gang's operation, but does not have the manpower she needs to carry out an extensive campaign. Even if she did, she doubts whether traditional foot and car patrols could safely put a stop to the gang's activities. The department has recently spent a considerable sum of money on investigative technology. The chief decides that using the new gadgets to identify and assemble evidence against the kingpins and soldiers of the operation would be the perfect way to prove the worth of the investment.

The attack against the gang proceeds on several fronts. Telephone poles at every intersection of Slumville are conspicuously outfitted with bullet-resistant video cameras, equipped with wide-angle lenses and 24-hour recording capacity. Miniature video cameras with pinhole apertures are covertly installed in a number of Slumville buildings thought to house gang members. At night, police periodically fly over the area in helicopters, armed with nightscopes that have a magnification capability of 500x and devices that detect heat waves emanating from buildings, a telltale sign of a drug processing laboratory.

Any car that leaves or enters the area is tracked electronically, following signals from transponders installed as part of Chicago's Intelligent Transportation System or, if the transponder has been removed, using signals from a beeper attached to the car by projectile launcher. At various streets leading into Slumville, checkpoints are established. At each one, the department installs devices that produce detailed pictures of objects concealed by clothing or car exteriors. Similar hand-held devices are used by foot and car patrols to scan passersby. As a final measure, the city contracts with the federal government to have photographs of Slumville taken whenever a satellite is within range; these pictures can be enhanced to highlight suspicious activity.

* * *

All of this technology exists today, albeit in differing stages of development. Some of it (e.g., beepers and video cameras) has been available to the police in some form for decades.[1] Other technologies (e.g., sensitive "see-through" technology and satellite photography) have only recently begun to find their way into the law enforcement arsenal,[2] partly as the result of the "peace dividend" associated with the end of the Cold War.[3] Although none of this technology is routinely used by the average police department at present, it is likely to become more prevalent as it becomes less expensive and better known.

Unfortunately, current law is ill-equipped to handle the issues raised by this merger of space-age science and modern-day law enforcement. Indeed, police use of this surveillance technology is virtually unregulated by either legislation or administrative rules. While judicial decisions have produced some useful criteria for deciding when and how to regulate technological investigation, courts have failed to produce a consistent or comprehensive approach to such regulation.[4]

In 1995, the American Bar Association began an effort to fill this void. In May of that year, the ABA's Criminal Justice Section established a Task Force on Technology and Law Enforcement.[5] Composed of judges, prosecutors, defense attorneys, privacy experts, national security experts, law professors, and representatives of federal and state law enforcement agencies,[6] the Task Force was initially directed to

---

1. *See, e.g.*, ALAN F. WESTIN, PRIVACY AND FREEDOM 173 (1967) (noting that according to a "thorough" 1957 study of local and state governmental surveillance, "tracking devices . . . and hidden cameras were widely used not only by urban police and prosecutors' offices but also by suburban departments, sheriffs' offices, state troopers, highway patrols, and state attorney-generals' [sic] offices, as well as some state regulatory agencies and legislative committees.").

2. *See, e.g.*, Fox Butterfield, *New Devices May Let Police Spot People on the Street Hiding Guns*, N.Y. TIMES, Apr. 7, 1997, at A1, A10 (noting law enforcement plans to install sensitive weapon-detection systems in prisons and courthouses, and describing research into devices that could detect weapons under clothing from up to 60 feet away); Krysten C. Kelly, Note, *Warrantless Satellite Surveillance: Will Our Fourth Amendment Privacy Rights Be Lost in Space?*, 13 J. MARSHALL J. COMPUTER & INFO. L. 729, 761 (1995) ("[L]aw enforcement agencies will eventually use the satellite in surveillance . . . .").

3. For instance, the fastest, longest-range detection device was developed by the U.S. Army. *See* Butterfield, *supra* note 2, at A10. Satellite photography was also developed for military purposes. *See* Kelly, *supra* note 2, at 730 nn.10-12.

4. *See infra* Part II.A.

5. Letter from William H. Jeffress, Jr., Chair of the ABA's Criminal Justice Standards Committee, to Sheldon Krantz, Chair of the Task Force (May 3, 1995) (on file with the *Harvard Journal of Law and Technology*) [hereinafter Jeffress Letter].

6. The Task Force originally consisted of nine members and eleven liaisons from various interested organizations. Membership changed over the two-year period of the Task Force.

Task Force Members: Sheldon Krantz, Chair, Piper & Marbury, Washington, DC; Walter Bruce Brownridge, General Counsel to the Cleveland Police Department, Cleveland,

review the ABA's Electronic Surveillance Standards.[7] These standards, which cover wiretapping and bugging, have not been substantially revised since 1978.[8] However, the ABA also recognized the need to expand the scope of these standards to reflect the development of other "advanced investigative tools" — tools that might require a rebalancing of "the need for aggressive law enforcement with privacy and freedom . . . considerations."[9]

To carry out this objective, the Task Force divided law enforcement surveillance practices into three conceptual categories: communications surveillance, physical surveillance, and transactional surveillance.[10] The

---

OH; the Honorable James G. Carr, Judge, U.S. District Court, Toledo, OH; Scott Charney, Chief, Computer Crime Unit, U.S. Department of Justice; Andrew Good, defense attorney, Silverglate & Good, Boston, MA; the Honorable Richard Huffman, Associate Justice, Fourth District Court of Appeal, San Diego, CA; Professor Wayne R. LaFave, University of Illinois College of Law, Champaign, IL; Marc Rotenberg, Director, Electronic Privacy Information Center, Washington, DC; Gail Thackeray, Deputy County Attorney, Phoenix, AZ.

Reporters: Professor Christopher Slobogin, University of Florida College of Law, Gainesville, FL; the Honorable Martin Marcus, Judge, Bronx County Supreme Court, Bronx, NY.

Liaisons: James M. Caterson, National District Attorneys Association; Ronald Goldstock, ABA Criminal Justice Section Council; Samuel A. Guiberson, ABA Criminal Justice Section Science and Technology Committee; Mary F. Harkenrider, U.S. Department of Justice; William J. Johnson, National Association of Police Organizations; Lionel Kennedy, National Security Agency; Albert J. Krieger, National Association for Criminal Defense Lawyers; Emil P. Moschella, Federal Bureau of Investigation; Eric M. Noonan, National Association of Attorneys General; Ronald L. Plesser, ABA Individual Rights and Responsibilities Section; Terrence Sheridan, Major Cities Chiefs Association; Jo-Ann Wallace, National Legal Aid and Defender Association; Daniel Weitzner, Center for Democracy and Technology (ad hoc liaison); R. Hackney Wiegmann, U.S. Department of Defense; Brad Wiegmann, U.S. Department of Defense (replacing R. Hackney Wiegmann); Stuart Wirtz, Federal Bureau of Investigation (replacing Emil P. Moschella).

7. STANDARDS FOR CRIMINAL JUSTICE § 2 (2d ed. 1980 & Supp. 1986) [hereinafter Electronic Surveillance Standards]. These standards originated in the AMERICAN BAR ASSOCIATION PROJECT ON MINIMUM STANDARDS FOR CRIMINAL JUSTICE, STANDARDS RELATING TO ELECTRONIC SURVEILLANCE (Tentative Draft 1968) [hereinafter PROJECT].

8. The Electronic Surveillance Standards were modified in 1978 (Kenneth J. Hodson, Chair, Standing Committee on Association Standards for Criminal Justice; Frank J. Remington, Chair, Task Force on Electronic Surveillance; James G. Carr, Reporter) and in 1986 (William H. Erickson, Chair, Standing Committee on Association Standards for Criminal Justice; Eugene Cerruti, Reporter). Both revisions consisted primarily of updating commentary, although the 1978 revision did result in some changes to black-letter standards as well.

9. Jeffress Letter, *supra* note 5, at 1.

10. The Task Force identified two other areas of concern: searches and seizures of computers, and encryption. The former focuses primarily on searches and seizures *of* technology, as opposed to searches and seizures *using* technology. Encryption involves the use of technology to *prevent* searches and seizures. Accordingly, these areas are not closely related to the three categories identified in the text.

term communications surveillance encompasses the real-time[11] interception of oral, written, and electronic communications using electronic or other means.[12] Physical surveillance involves the real-time observation or detection of movements, activities, and conditions. Finally, transactional surveillance refers to efforts to access pre-existing records such as phone logs, electronic mail logs, credit card histories, other financial transaction data, and air, train, and bus travel bookings.[13]

This Article describes the ABA's current efforts to establish guidelines for technologically-assisted physical surveillance (i.e., physical surveillance that uses the types of technology described earlier). The Appendix sets out the Tentative Draft Standards Concerning Technologically-Assisted Physical Surveillance that were approved by the Task Force in February, 1997.[14] The body of the Article explains the process by which these standards were created. Part II describes and analyzes current law on the subject. Part III outlines the Task Force's current approach to technologically-assisted physical surveillance. Part IV identifies the issues that generated the most debate within the Task Force and explains how they were resolved.[15] The primary purposes of this Article are to alert interested parties (including law enforcement officials, lawyers, and the public) to the ABA's efforts and to encourage feedback.

---

11. The term "real-time" describes activities that occur in the present according to a conventional human time frame. With regard to communication, "real-time" surveillance occurs contemporaneously; it does not include searches of records of past transactions.

12. Standards on this topic are currently being revised by the Task Force, with the Honorable Martin Marcus as Reporter.

13. *See generally* Jonathan P. Graham, Note, *Privacy, Computers, and the Commercial Dissemination of Personal Information*, 65 TEX. L. REV. 1395, 1397-1402 (1987). Although this information can be accessed through traditional means, computers greatly facilitate "collecting, storing, processing and disseminating personal data." *Id.* at 1397. Given resource and time constraints, the Task Force is not likely to develop standards in this area.

14. As the title indicates, these standards are only preliminary. Although the Task Force has approved them, to become official ABA policy they must be endorsed by a majority of the ABA House of Delegates. Before that can occur, the standards and accompanying commentary must be reviewed by the Criminal Justice Standards Committee (a group of judges, defense attorneys, and prosecutors) and the standards (*sans* commentary) must be reviewed and approved by the Criminal Justice Section Council (a similarly-constituted group), with the latter subjecting the standard to two formal readings.

15. Although a commentary to the Tentative Draft Standards exists, it is not reproduced here for several reasons. First, it is still in draft form, as it must be because significant changes to the standards could occur. *See supra* note 14. Second, even the draft version is extremely long. Third, the ABA retains copyright over the commentary. Nonetheless, the overlap between the draft commentary and this Article is significant, if only because the two documents have the same author.

II. THE LEGAL RESPONSE TO PHYSICAL SURVEILLANCE

To the extent any regulation of law enforcement use of technologically-assisted physical surveillance has occurred, it has come primarily from courts. In contrast to electronic surveillance of communications[16] and some types of transactional surveillance,[17] physical surveillance has never been the subject of concerted legislative oversight. Neither the ABA's Electronic Surveillance Standards[18] nor the analogous federal provisions dealing with electronic surveillance (Title III) regulate technological enhancement of physical surveillance.[19] State and local lawmaking bodies have also largely avoided the issue.[20]

Courts, on the other hand, have been increasingly active in setting legal parameters for the use of these surveillance devices. Judicial analysis has focused on whether, and to what extent, the Fourth Amendment is implicated by physical surveillance. The initial question under that Amendment has been whether the surveillance is a "search." Since *Katz v. United States*,[21] in which the Supreme Court held that police use of a bugging device to eavesdrop on a phone booth conversation is a Fourth Amendment search, this threshold has been defined as police action that infringes on "expectation[s] of privacy . . .

---

16. *See* Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510-2520 (1994) [hereinafter Title III]. Since the enactment of the 1968 Act, there have been two significant amendments to Title III: the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified in scattered sections of 18 U.S.C.) (regulating, *inter alia*, the interception of cellular phone calls and electronic mail) and the Digital Telephony Act of 1994, Pub. L. No. 103-414, 108 Stat. 4279 (codified at 47 U.S.C. §§ 1001-1010 (1994 & Supp. 1997) and in scattered sections of 18 U.S.C.) (dealing primarily with the configuration of communications systems to facilitate access by law enforcement).

17. For example, the Electronic Communications Privacy Act regulates access to stored electronic communications and electronic bulletin board member lists. *See* 18 U.S.C. § 2703(c)(1)(A) (1994). The Right to Financial Privacy Act regulates access to financial information. *See* 12 U.S.C. § 3402 (1994). The Cable Television Privacy Act regulates disclosure of identifying information about cable subscribers. *See* 47 U.S.C. § 551 (1994).

18. As the commentary to the Project stated, "[I]t was felt that the standards should be limited to aural surveillance, since it was in this field that we had the greatest experience and that to attempt to go beyond that experience now would be premature." PROJECT, *supra* note 7, at 104.

19. *But see infra* text accompanying note 94.

20. *See, e.g.*, Richard Cole, *Man with Hidden Camcorder May Be Guilty, But of What?*, SAN DIEGO UNION-TRIB., Mar. 26, 1996, at A3 (reporting that surreptitious filming of private club members is not a crime unless simultaneous audio recording occurs). *But cf.* SEMINOLE COUNTY FLORIDA, SEMINOLE COUNTY FLORIDA TRAFFIC MANAGEMENT SYSTEM POLICY FOR USE OF TRAFFIC MONITORING DEVICES (1996) (on file with the *Harvard Journal of Law and Technology*) (detailing regulations that govern public use of video cameras by law enforcement agencies).

21. 389 U.S. 347 (1967).

that society is prepared to recognize as 'reasonable.'"[22] Assuming surveillance does implicate the Fourth Amendment, the second question concerns the criteria necessary to authorize surveillance — a warrant based on probable cause, something more, or something less. One of the Task Force's first tasks was to analyze judicial treatment of these issues with respect to physical surveillance.

A. Factors from the Case Law

In deciding whether a particular type of physical surveillance is a search and, if so, how to regulate it, the courts have adopted a multi-factor approach. The seven factors discussed below overlap to some extent; further, in any given case only a few may be explicitly mentioned. Considered together, however, they span the universe of considerations that courts have applied to physical surveillance, whether or not it is technologically-aided.

1. The Nature of the Place To Be Observed

The most important factor has been the nature of the place subjected to physical surveillance. Not surprisingly, given *Katz*'s emphasis on expectations of privacy, enhanced surveillance is least likely to be left unregulated when it focuses on the home, normally the site of one's most intimate activities. Thus, courts often hold that observing the interior of a home or similar area[23] is a search, at least when conducted with enhancement devices.[24] In such instances, courts usually require a

---

22. *Id.* at 361.

23. *Katz*'s holding that bugging a phone booth is a search established that while homes may be the paradigmatic protected area, certain other areas are entitled to substantial protection. *See, e.g.*, O'Connor v. Ortega, 480 U.S. 709 (1987) (holding that desk drawers in an office are entitled to a reasonable expectation of privacy); State v. Bryant, 177 N.W.2d 800 (Minn. 1970) (holding that restrooms in a store are protected by the Fourth Amendment); Alward v. State, 912 P.2d 243 (Nev. 1996) (finding a reasonable expectation of privacy in a tent, even though positioned on public land); State v. Baker, 271 A.2d 435 (N.J. 1970) (finding that a private room in a store is protected by the Fourth Amendment).

24. *See, e.g.*, United States v. Taborda, 635 F.2d 131 (2d Cir. 1980) (observation of a residence using a telescope); United States v. Kim, 415 F. Supp. 1252 (D. Haw. 1976) (same); State v. Ward, 617 P.2d 568 (Haw. 1980) (same); State v. Blacker, 630 P.2d 413 (Or. Ct. App. 1981) (same); State v. Crea, 233 N.W.2d 736 (Minn. 1975) (shining a flashlight into a basement); Commonwealth v. Williams, 431 A.2d 964 (Pa. 1981) (observation of an apartment using binoculars and a Startron nightscope); *see also* WAYNE LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 2.2 (3d ed. 1996). As Professor LaFave notes, when the surveillance is with the naked eye, a different view prevails: "At least when the officer only employs his natural senses, the prevailing rule is that such uses of the senses 'made from a place where a police officer has a right to be do not amount to a search in the constitutional sense.'" *Id.* at § 2.3(c) (citations omitted).

warrant based on probable cause, although in some situations more might be required and in others less might be sufficient. For example, many lower courts have held that video surveillance of the interior of a home must meet the more stringent federal statutory requirements applied in the wiretapping context.[25] Toward the other end of the spectrum, in *United States v. Karo*,[26] the Supreme Court held that the use of an electronic beeper to detect movement within a house is a search that requires some type of judicial authorization, but left open the question of whether probable cause or merely reasonable suspicion is required.[27] As developed below,[28] many lower courts have held that even *suspicionless* surveillance of homes is permitted under certain circumstances. Nonetheless, as a general rule courts accord homes and like areas the most significant protection.

In contrast, when the surveillance is of an area outside a residence or similarly private area, courts have often found the Fourth Amendment irrelevant. For instance, the Supreme Court held in *United States v. Knotts*[29] that use of a beeper to detect movement on the public roads is not a search. Also not a search, according to the Court, is the use of an illumination device to inspect the interior of a car through a window,[30] the interior of a barn located in an open field,[31] or the exterior of a boat.[32] Nor is aerial surveillance of industrial[33] or residential[34] curtilage normally a search, even if it takes place only 400 yards above the ground.[35] Consonant with these Supreme Court opinions, lower courts have typically held that the use of enhancement devices to view cars, curtilage, open fields, or public areas is not a search.[36]

---

25. *See, e.g.*, United States v. Torres, 751 F.2d 875 (7th Cir. 1984) (holding that a Title III warrant describing with particularity the place to be viewed is necessary to authorize video surveillance, and may be issued only if other means of investigation have failed and steps are taken to minimize unnecessary privacy intrusions); United States v. Falls, 34 F.3d 674 (8th Cir. 1994); United States v. Koyomejian, 970 F.2d 536 (9th Cir. 1992).

26. 468 U.S. 705 (1984).

27. *See id.* at 718.

28. *See infra* notes 39, 56-57 & 62 and accompanying text (discussing cases that involve a failure to take precautions, the use of "common" technology, and confirmation of naked-eye viewing).

29. 460 U.S. 276 (1983).

30. *See* Texas v. Brown, 460 U.S. 730 (1983).

31. *See* United States v. Dunn, 480 U.S. 294 (1987).

32. *See* Lee v. United States, 274 U.S. 559 (1927).

33. *See* Dow Chem. Co. v. United States, 476 U.S. 227 (1986) (a telescopic map-making camera in aerial surveillance).

34. *See* California v. Ciraolo, 476 U.S. 207 (1986).

35. *See* Florida v. Riley, 488 U.S. 445 (1989) (low-altitude helicopter surveillance).

36. *See* LAFAVE, *supra* note 24, § 2.2(b)-(c).

2. The Steps Taken to Enhance Privacy

Even an area normally associated with an expectation of privacy may not be entitled to Fourth Amendment protection if no efforts are made to keep it private. Thus, in holding a flashlight inspection of a barn to be outside the Fourth Amendment's purview, the Supreme Court's decision in *United States v. Dunn*[37] noted that the upper portion of a "wall" through which police observed the interior consisted only of netting material.[38] Similarly, in *California v. Ciraolo*,[39] the fact that the defendant's fence was only ten feet high, and thus would not have kept observers on a truck or a double-decker bus from seeing his backyard helped justify aerial surveillance of residential curtilage. In a like vein, lower courts have often considered the presence of fences and curtains, the height of windows, and whether objects were out of the line of normal sight.[40] In short, a lack of effort to protect privacy may mean that one does not have any for Fourth Amendment purposes.

3. The Degree to Which the Surveillance Requires a Physical Intrusion onto Private Property (i.e., the Location of the Observer)

In finding that no search had occurred in *Ciraolo* and its companion case, *Dow Chemical Company v. United States*,[41] the Court emphasized the fact that the government had flown over the land rather than physically intruded upon it.[42] Similarly, a dog sniff of luggage is not a search in part because the dog itself does not intrude into the luggage.[43] Lower courts have echoed the view, which harkens back to pre-*Katz*

---

37. 480 U.S. 294 (1987).

38. *See id.* at 298.

39. 476 U.S. 207 (1986).

40. *See, e.g.*, People v. Ferguson, 365 N.E.2d 77 (Ill. App. Ct. 1977) (holding that the use of binoculars to look through the windows of a second floor apartment from 60 feet away is not a search); People v. Hicks, 364 N.E.2d 440 (Ill. App. Ct. 1977) (holding that the use of night binoculars to look into a first-floor hotel room when curtains could have been pulled is not a search); State v. Littleton, 407 So.2d 1208 (La. 1981) (holding that the use of binoculars to look into a hangar with a thirty- to forty-foot-wide opening is not a search); State v. Louis, 672 P.2d 708 (Or. 1983) (holding that the use of a telephoto lens to observe a person repeatedly positioning himself at a window is not a search).

41. 476 U.S. 227 (1986).

42. *See Ciraolo*, 476 U.S. at 207 ("The observations . . . took place within public navigable airspace . . . in a physically nonintrusive manner . . . ."); *Dow Chem.*, 476 U.S. at 237 ("The narrow issue . . . concerns aerial observation of a 2,000-acre outdoor manufacturing facility *without* physical entry.").

43. *See* United States v. Place, 462 U.S. 696, 707 (1983) (holding that because a dog sniff "does not require opening the luggage [and] does not expose noncontraband items that otherwise would remain hidden from public view . . . this investigative technique is much less intrusive than a typical search").

trespass analysis,[44] that the absence of an intrusion diminishes Fourth Amendment concerns. For instance, courts have sanctioned the use of thermal-imaging devices to detect heat waves emanating from houses in part because the surveillance does not require an entry.[45]

A closely related issue is whether the observer's vantage point is "lawful"; this question is usually simply another way of asking whether the surveillance involves an intrusion into private space. Even private property can be a lawful vantage point, as demonstrated by the holding in *Dunn* that viewing the interior of a structure from a privately-owned open field is not a search[46] and by lower court rulings that viewing the interior of a home from that part of the curtilage that invites the public (e.g., a sidewalk) is not a search.[47] On the other hand, sufficiently unusual vantage points, including those located in public space, may not be "lawful" for Fourth Amendment purposes.[48] When a vantage point *is* lawful, however, even surveillance using enhancement devices is often found to be acceptable — several courts have held, for instance, that so long as the vantage point is lawful, using binoculars to look into a private residence is not a search.[49]

4. The Nature of the Object or Activity Observed

In *Ciraolo*, the Court stated that *Katz*'s rule protecting the privacy of conversations "does not translate readily into a rule of constitutional

---

44. Prior to *Katz*, Fourth Amendment protection depended upon whether police actions constituted a trespass on the property of the suspect. *See* Olmstead v. United States, 277 U.S. 438 (1928) (holding that tapping telephone wires outside suspects' premises is not a search); Goldman v. United States, 316 U.S. 129 (1942) (holding that listening to a conversation in an adjoining room by means of a "detectaphone" placed against the wall is not a search).

45. *See, e.g.*, United States v. Pinson, 24 F.3d 1056, 1059 (8th Cir. 1994) ("The detection of the heat waste was not an intrusion into the home; no intimate details of the home were observed, and there was no intrusion upon the privacy of the individuals within."); United States v. Ishmael, 48 F.3d 850, 856 (5th Cir. 1995) (finding that thermal imaging devices do not in "any way penetrate structures within [the] area").

46. *See* United States v. Dunn, 480 U.S. 294, 304-05 (1987).

47. *See* LAFAVE, *supra* note 24, § 2.3(c).

48. *See* State v. Kender, 588 P.2d 447 (Haw. 1978) (holding that a search occurs where an officer climbs three-quarters of the way up a fence and braces himself on a fellow officer's shoulder to use a telescope to see into a backyard).

49. *See, e.g.*, United States v. Whaley, 779 F.2d 585 (11th Cir. 1986) (holding that the use of binoculars to observe a basement through a window from neighboring property is not a search); People v. Ferguson, 365 N.E.2d 77 (Ill. App. Ct. 1977); People v. Hicks, 364 N.E.2d 440 (Ill. App. Ct. 1977); State v. Littleton, 407 So.2d 1208 (La. 1981); State v. Thompson, 241 N,W.2d 511 (Neb. 1976) (holding that the use of binoculars to observe a living room from an alley where "officers had a right to be" is not a search); State v. Louis, 672 P.2d 708 (Or. 1983).

dimensions that one who grows illicit drugs in his backyard" is entitled to an expectation of privacy.[50] Along the same lines, the Court has held that testing a substance strongly believed to be cocaine is not a search,[51] nor is a dog sniff of luggage that which alerts the police only to the presence of contraband.[52] Observation of impersonal objects other than illicit substances may also be less subject to regulation. In *Dow Chemical,* the Court noted that the aerial photographs in dispute revealed physical details of Dow's plant, but not "identifiable human faces or secret documents," or other "intimate details."[53] Similarly, several cases holding that the use of thermal imaging devices is not a search characterize heat waves as "waste."[54]

5. The Availability of the Technology to the General Public

The camera used in *Dow Chemical* had a magnification capability of 240x[55] and cost $22,000. These facts did not give the Court pause, because the camera could be purchased on the commercial market.[56] The Court, however, added that the same observation "using highly sophisticated surveillance equipment not generally available to the public, such as satellite technology, might be constitutionally proscribed absent a warrant."[57] Further, the use of "an electronic device to penetrate walls or windows so as to hear and record confidential discussions of chemical formulae or other trade secrets would raise very different and far more

---

50. California v. Ciraolo, 476 U.S. 207, 214 (1986). Presumably for the same reason a burglar has no expectation of privacy. *Cf.* Rakas v. Illinois, 439 U.S. 128, 143 n.12 (1978) ("A burglar plying his trade in a summer cabin during the off season may have a thoroughly justified expectation of privacy, but it is not one which the law recognizes as 'legitimate.'").

51. *See* United States v. Jacobsen, 466 U.S. 109, 123 (1984) ("Congress has decided ... to treat the interest in 'privately' possessing cocaine as illegitimate; thus, governmental conduct that can reveal whether a substance is cocaine, and no other arguably 'private' fact, compromises no legitimate privacy interest.").

52. *See* United States v. Place, 462 U.S. 696, 707 (1983) ("The sniff discloses only the presence or absence of narcotics, a contraband item. Thus, despite the fact that the sniff tells the authorities something about the contents of the luggage, the information obtained is limited.").

53. Dow Chem. Co. v. United States, 476 U.S. 227, 239 n.5 (1986).

54. *See* United States v. Pinson, 24 F.3d 1056, 1059 (8th Cir. 1994); United States v. Penny-Feeney, 773 F. Supp. 220, 225 (D. Haw. 1991).

55. *See Dow Chem.*, 476 U.S. at 242-43 & n.4 (Powell, J., dissenting) (finding that the camera allowed "enlargement to a scale of 1 inch equals 20 feet or *greater*, without significant loss of detail or resolution") (emphasis added).

56. *See id.* at 238 (describing the camera as "a conventional, albeit precise, commercial camera commonly used in map-making").

57. *Id.*

serious questions" than the camera surveillance in *Dow Chemical*.[58] Lower courts have echoed these sentiments, quite often finding the commonness of the surveillance technique to be dispositive.[59]

The reasoning in these cases takes on the flavor of the Supreme Court's undercover investigation jurisprudence,[60] in which the targets of surveillance are said to assume the risk that the people with whom they interact will be government agents. In this context, however, the risk said to be assumed is actually twofold. First, these courts are saying that we must assume the risk that any device which is readily available on the market will be used to observe our movements and activities. Second, they are saying that, just as we should know that an acquaintance may be working for law enforcement, we assume the risk that those using such enhancement devices are government agents.

6. The Extent to Which the Technology Enhances the Natural Senses

Some courts have distinguished between devices that "improve" human senses and devices that "replace" them, with the latter being more likely to implicate the Fourth Amendment.[61] Using the examples given

---

58. *Id.* at 239.

59. *See, e.g.*, United States v. Allen, 675 F.2d 1373, 1380 (9th Cir. 1980) (holding that the use of a special lens is not a search because "such equipment is widely available commercially"); State v. Vogel, 428 N.W.2d 272, 275 (S.D. 1988) (finding no search where a camera with a zoom lens is used to photograph the interior of a residence and there is "no showing that the cameras and lenses used . . . [are] 'sophisticated visual aids' or 'special equipment not generally in use'"); State v. Rose, 909 P.2d 280, 286 (Wash. 1996) (holding that the use of a flashlight to look into a house is not a search in part because a flashlight is "an exceedingly common device"); State v. Lange, 463 N.W.2d 390 (Wis. Ct. App. 1990) (finding no search when standard binoculars and cameras equipped with generally available standard and zoom lenses are used to view homes).

60. *See, e.g.*, Lewis v. United States, 385 U.S. 206, 211 (1966) (holding that entry into a home by an undercover agent posing as a drug dealer is not a search when defendant invites him); United States v. White, 401 U.S 745, 752 (1971) (holding that taping a conversation using a body bug on a government informant is not a search because there is no significant difference between recording and hearing statements); United States v. Miller, 425 U.S. 435, 443 (1976) (holding that a government subpoena of bank records is not a search because a depositor "takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the government"); Smith v. Maryland, 442 U.S. 735, 743-44 (1979) (holding that obtaining a defendant's phone numbers from the phone company is not a search because a person has no expectation of privacy "in information he voluntarily turns over to third parties").

61. *Compare* People v. Arno, 153 Cal. Rptr. 624, 626 (Ct. App. 1979) (finding that binoculars may be used "to permit clandestine police surveillance of that which could be seen from a more obvious vantage point without the optical aid") *with* United States v. Thomas, 757 F.2d 1359, 1367 (2d Cir. 1985) (finding that the use of a dog is "not a mere improvement of sense of smell, as ordinary eyeglasses improve vision, but is a significant enhancement accomplished by a different, and far superior, sensory instrument").

in *Dow Chemical*, a satellite or gadget that sees through walls could be said to replace one's senses rather than enhance them because it sees things that the police might never be able to see with the eye. Conversely, when enhancement devices simply "confirm" something already seen by the naked eye, or see something that could be viewed with the naked eye but for fear of discovery, the use is less likely to be seen as a search, even if the surveillance is of the home.[62] This idea may help explain the holding in *Texas v. Brown*,[63] where the Supreme Court upheld the warrantless use of a flashlight to search the interior of a car, stating that "the use of artificial means to illuminate a darkened area simply does not constitute a search, and thus triggers no Fourth Amendment protection."[64]

7. The Extent to Which the Surveillance Is Unnecessarily Pervasive, Invasive, or Disruptive (i.e., Steps Taken to Minimize the Intrusion)

Finally, several courts addressing the propriety of physical surveillance have considered a complex of factors analogous to those associated with minimization in the electronic surveillance context.[65] Most significantly, they have looked at the number of people or objects observed (the pervasiveness issue). For instance, while lower courts accept the idea that a dog sniff of luggage is generally not a search, several have expressed concern over the routine use of dogs to sniff all packages in a particular area.[66] Similarly, while aerial surveillance is generally not considered a search, courts have condemned random aerial patrols over wide-ranging areas.[67] Along the same lines, in his dissent

---

62. *See* United States v. Bassford, 601 F. Supp. 1324, 1335 (D. Me. 1985), *aff'd*, 812 F.2d 16 (1st Cir. 1987) (holding that the use of binoculars is not a search when they give a "view of a readily visible marijuana plot previously observed with the naked eye"); State v. Holbron, 648 P.2d 194, 197 (Haw. 1982) (finding no search where binoculars are used only to confirm unaided observations); State v. Irwin, 718 P.2d 826, 829-30 (Wash. Ct. App. 1986) (holding that the use of an enhancement device from nearby woods in order to avoid detection is not a search).

63. 460 U.S. 730 (1983).

64. *Id.* at 740.

65. *See* 18 U.S.C. § 2518(5) (1994) (stating that electronic surveillance "shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter . . .").

66. *See, e.g.*, United States v. Beale, 674 F.2d 1327, 1336 (9th Cir. 1982), *vacated*, 463 U.S. 1202 (1983) ("Nothing would invoke the specter of a totalitarian police state as much as the indiscriminate, blanket use of trained dogs at roadblocks, airports and train stations."); United States v. Whitehead, 849 F.2d 849, 857 (4th Cir. 1988) ("*Place* obviously did not sanction the indiscriminate, blanket use of trained dogs in all contexts.").

67. *See* State v. Riley, 511 So.2d 282, 287-89 (Fla. 1987), *rev'd*, 488 U.S. 445 (1989) (finding that low-level, indiscriminate helicopter surveillance is a search); People v. Agee, 200 Cal. Rptr. 827, 836 (Cal. Ct. App. 1984) (criticizing wide-ranging aerial surveillance

in *Jacobsen*, Justice Brennan cautioned against reading the Court's contraband search cases to permit police dogs to "roam the streets at random, alerting officers to people carrying cocaine," to allow drug scanning devices to "scan . . . all passersby," or to authorize the use of such devices "to identify all homes in which [contraband] is present."[68]

Conversely, "dragnet" use of such methods in a context of well-recognized danger (e.g., magnetometers in an airport) might be enthusiastically welcomed.[69] In this type of situation, courts have recognized that the pervasiveness of the search may make it *less* invasive;[70] in other words, subjecting everyone to a search may create less of a sense of oppression or intrusion than singling out particular individuals without suspicion.

The duration of the surveillance and its intensity are also relevant to the invasiveness issue. Courts have leveled criticism at prolonged observation[71] and at observation that is insufficiently limited in objective.[72] A few courts have also expressed concern about "blanket" surveillance under which a target's every public movement is conspicuously observed.[73]

Finally, the disruptiveness of the surveillance might be a factor. In *Florida v. Riley*,[74] the Supreme Court suggested that low-altitude, aerial surveillance might become a search if conducted with "hazard to persons or property on the surface" or in a way that interferes with "normal use

---

as a police-state tactic).

68. United States v. Jacobsen, 466 U.S. 109, 138 (1984) (Brennan, J., dissenting). *But see* Davis v. Mississippi, 394 U.S. 721, 727-28 (1969) (noting that dragnet seizures of people to obtain fingerprints might be reasonable if done in a manner that is not overly invasive).

69. *See* Christopher Slobogin, *The World Without a Fourth Amendment*, 39 UCLA L. REV. 1, 62-63 (1991).

70. *See, e.g.*, Delaware v. Prouse, 440 U.S. 648, 663 (1979) (finding that while random stops are impermissible, the "[q]uestioning of all oncoming traffic at roadblock-type stops is one possible alternative"). At least one court has recognized that "[i]t is not necessary for a checkpoint to stop every car in order to be systematic but only for officers to be following some pattern that will minimize their discretion in choosing whether to stop a particular auto." People v. Estrada, 386 N.E.2d 128, 130 (Ill. App. Ct. 1979).

71. *See, e.g.*, Commonwealth v. Williams, 431 A.2d 964, 966 (Pa. 1981) (involving officers who observed the interior of a home, including private sexual conduct, for nine days using binoculars and a nightscope).

72. *See, e.g.*, Smayda v. United States, 352 F.2d 251, 257 (9th Cir. 1965) (requiring that observations be limited "to the times when [restroom] crimes are most likely to occur").

73. *See, e.g.*, McGee v. Hester, 724 F.2d 89, 90-92 (8th Cir. 1983) (holding that open and excessive surveillance is grounds for a civil rights action when it diminishes store sales). *But cf.* United States v. Knotts, 460 U.S. 276, 284 (1983) (responding to the argument that unlimited beeper surveillance is unconstitutional, the Court stated: "if such dragnet type law enforcement practices . . . should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable.").

74. 488 U.S. 445 (1989).

of the [home] . . . or curtilage."[75] Lower courts also have looked at the altitude of the aircraft and resulting disruption.[76] One could imagine similar considerations affecting the propriety of the use of other types of surveillance such as aggressive, overt use of video cameras to record a political meeting.

B. Analysis of the Factors

The multiplicity of factors considered by courts in deciding the scope of the Fourth Amendment's application to physical surveillance makes any clear statement of the law in this area difficult. Nonetheless, the Task Force eventually concluded that some sort of multi-factor approach is both inevitable and proper given the elusive nature of the privacy concept.[77] Indeed, Standard 2-6.1(c)(ii) essentially replicates the seven factors described above and adds a few of its own.

At the same time, several of the factors identified by the courts are probably entitled to very little weight as a matter of constitutional law or policy. While factors (1) and (7), dealing with the place observed and the minimization concept, respectively, seem central to any analysis of physical surveillance technology, the other factors' relevance to this endeavor are suspect to varying degrees. A brief survey of the ways in which these remaining five factors are deficient aids the evaluation of the case law and the standards.

Factor (2), which focuses on ease of observation, is suspect for two reasons. First, it is troublesome to the extent it affords less protection to those who, for economic or other uncontrollable reasons, cannot take steps to protect their privacy.[78] More importantly, as many have pointed out, basing the degree of protection from government surveillance on

---

75. *Id.* at 451-52.

76. *See, e.g.*, Gianocola v. West Va. Dept. of Pub. Safety, 830 F.2d 547, 550-51 (4th Cir. 1987) (considering the effect of aerial surveillance on ground activity); People v. Sneed, 108 Cal. Rptr. 146, 151 (Ct. App. 1973) ("[The defendant had] a reasonable expectation of privacy to be free from noisy police observation by helicopter from the air at 20 to 25 feet and that such an invasion was an unreasonable governmental intrusion into the serenity and privacy of his backyard."); State v. Rogers, 673 P.2d 142, 143 (N.M. Ct. App. 1983) ("[C]ourts have considered . . . altitude of the aircraft, use of equipment to enhance the observation, frequency of other flights and intensity of the surveillance.").

77. *See infra* Part IV.C.2.

78. *See* Ronald J. Bacigal, *Some Observations and Proposals on the Nature of the Fourth Amendment*, 46 GEO. WASH. L. REV. 529, 541-42, 542 nn.94-95 (1978) (noting that privacy exists only for "those wealthy enough to live exclusively in private places"); Kenneth Troiano, Comment, *Law Enforcement Use of High Technology: Does Closing the Door Matter Anymore?*, 24 CAL. W. L. REV. 83, 92 (1988) (noting that only professional criminals and the wealthy can afford the technology to hide from high technology surveillance).

efforts to evade it runs the risk of fostering a closed society in which people routinely curtail contact with the outside world.[79] The advent of highly intrusive technologies exacerbates this risk, since increasing levels of precaution (e.g., thicker walls, heavily curtained windows, and avoidance of public exposure) are necessary to render them ineffective.

Factor (3), the location of the observer, should also at most be a secondary consideration in privacy analysis. As with factor (2), those with less wherewithal may have reduced protection from surveillance simply because they cannot distance themselves from lawful vantage points. More importantly, the location of the observer may often have little to do with the degree of privacy intrusion. Surveillance of one's bedroom (or one's closed-in backyard) is equally intrusive whether conducted via binoculars or by an officer who has trespassed and remains hidden from view. Indeed, attributing significance to physical intrusion may encourage the police to engage in "non-physical" searches that are actually more intrusive.[80]

Factor (4), the object(s) of the surveillance, is of questionable relevance to the extent it forces distinctions between "intimate" and "non-intimate" objects — into which category does one place clothing, book covers, or unoccupied living rooms? Even if the factor is refocused on whether the object is contraband, it remains suspect to the extent it permits dragnet searches of the type described by Justice Brennan in his *Jacobsen* dissent.[81] On the other hand, if limited by factor (7), the minimization factor, whether surveillance reveals only illicit items may be an important and useful variable in expectation of privacy analysis.[82]

---

79. *See, e.g.*, Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 402 (1974).

> [S]o far as I am presently advised of the state of the mechanical arts — anyone can protect himself against surveillance by retiring to the cellar, cloaking all the windows with thick caulking, turning off the lights and remaining absolutely quiet. This much withdrawal is not required in order to claim the benefit of the Amendment because, if it were, the Amendment's benefit would be too stingy to preserve the kind of open society to which we are committed and in which the Amendment is supposed to function.

Id. at 402; *see also* Robert C. Power, *Technology and the Fourth Amendment: A Proposed Formulation for Visual Searches*, 80 J. CRIM. L. & CRIMINOLOGY 1, 38-39 (1989) ("Whatever the Supreme Court meant by the reasonable expectation of privacy in *Katz*, it could not have anticipated that the term would be turned around and used to mandate nearly absolute security before Fourth Amendment protection attaches.").

80. *See* David E. Steinberg, *Making Sense of Sense-Enhanced Searches*, 74 MINN. L. REV. 563, 591 (1990).

81. *See supra* text accompanying note 68.

82. *Cf.* Arnold H. Loewy, *The Fourth Amendment as a Device for Protecting the Innocent*, 81 MICH. L. REV. 1229, 1246-48 (1983); Richard G. Wilkins, *Defining the "Reasonable Expectation of Privacy": An Emerging Tripartite Analysis*, 40 VAND. L.

Factor (5), the availability of the technology to the public, is flawed because of its close association with the assumption of risk rationale, which many commentators consider to be tautological: in a real sense, we only assume those risks of unregulated government intrusion that the courts tell us we have to assume.[83] Left on our own, our "assumptions" about what types of enhancement devices we expect to be used, and by whom, might be quite different from what the courts tell us they should be.[84] Furthermore, giving full weight to this factor would eliminate privacy expectations even in much of the home because so many highly intrusive devices (e.g., $22,000 map-making cameras) are readily "available" to the public.

Factor (6), whether a device replaces, rather than enhances naked-eye observation, may ultimately be premised on a false distinction. Presumably, if the enhancement device does not in some way "replace" police vision, it will not be used in the first place. If, for instance, the police in *Knotts*[85] could have tailed the suspect's car without using a beeper, why didn't they?[86] In the "confirmation" cases,[87] if the police could see into the premises with the naked eye, why were enhancement devices used? In each case, the device was apparently viewed as a more efficient, but not necessary, way of pursuing the police investigation.

REV. 1077, 1121-28 (1987); Steinberg, *supra* note 80, at 617.

83. As Professor Coombs states: "Once we decide the parameters of the government's power, the claimant 'assumes' whatever risk inheres in that legal rule." Mary I. Coombs, *Shared Privacy and the Fourth Amendment, or the Rights of Relationships*, 75 CAL. L. REV. 1593, 1643 (1987); *see also* Melvin Gutterman, *A Formulation of the Value and Means Models of the Fourth Amendment in the Age of Technologically Enhanced Surveillance*, 39 SYRACUSE L. REV. 647, 670 (1988) ("[The] 'assumption of risks' [analysis] . . . miss[es] the mark. . . . It overlook[s] the central issue, the significance of . . . surveillance as a threat to our sense of security.").

84. In a study I conducted with Joseph Schumacher, subjects asked to rate the "intrusiveness" of fifty different search scenarios frequently disagreed with the Supreme Court's conclusions about expectations of privacy. *See* Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society"*, 42 DUKE L.J. 727, 740-42 (1993). For instance, while the Court has held that a dog sniff, *see* United States v. Place, 462 U.S. 696 (1983), and a trespass on open fields, *see* Oliver v. United States, 466 U.S. 170 (1984), are not searches, the subjects in the study saw these actions to be as intrusive as a frisk, which the Court held is a search in Terry v. Ohio, 392 U.S. 1 (1968). *See* Slobogin & Schumacher, *supra*, at 737-41.

85. United States v. Knotts, 460 U.S. 276 (1983).

86. As one court has stated, if a beeper simply permits the police to do more easily what they could accomplish with the naked eye, "then there is no need for the device in the first place. Its value lies in its ability to convey information not otherwise available to the government." United States v. Holmes, 521 F.2d 859, 866 n.13 (5th Cir. 1975), *aff'd en banc by an equally divided court*, 537 F.2d 227 (5th Cir. 1976).

87. *See supra* note 62 and accompanying text.

A hypothetical, but not unrealistic,[88] example illustrates the insidious effect of incautiously applying these five factors. Suppose the police, while hiding in bushes at the edge of a farm, use a nightscope with magnification capability to look in a darkened bedroom window located on the second story of a house 500 yards away. Given its location (factor (1)), the bedroom is presumptively entitled to Fourth Amendment protection, especially if the surveillance is prolonged (factor (7)). But suppose the window curtains are not drawn (factor (2)); the police do not move beyond the edge of the property (factor (3)); the only items actually spied are contraband and furniture (factor (4)); the nightscope is commercially available, albeit costly[89] (factor (5)); and the police are worried that closer, unaided viewing would give away their presence (factor (6)). A strong case can then be made that the action is not a search. That result should not be countenanced, as it would allow police to engage in such conduct at random, without developing any degree of suspicion or seeking authorization from a magistrate.[90]

C. The Narrowness of the Case Law

In short, many of the factors that courts consider in the regulation of physical surveillance are of dubious value.[91] Insufficient sensitivity to this fact is not the only failing of the case law, however. As might be expected from a decisionmaking process that requires a case and controversy and is focused on constitutional doctrine, the case law leaves

---

88. *See* United States v. Lace, 669 F.2d 46, 53 (2d Cir. 1982) (Newman, J., concurring) (involving continuous covert surveillance of the curtilage from private property using a Bushnell spotting scope with 45x magnification, a Questar lens with 130x magnification, infrared goggles, and a Javelin nightscope capable of magnifying existing light 50,000 times; in dicta the majority stated that this was not an invasion of a reasonable expectation of privacy protected under the Fourth Amendment).

89. A hand-held Vacro Noctron V scope costs about $3,300. A Startron Headstone (a nightscope mounted on a headset) costs about $4,200. *See* Mike Cook, *Scopes for Nighttime Use a Valuable Tool for Louisiana Department of Wildlife and Fisheries*, BATON ROUGE ST. TIMES, Jan. 8, 1991, at 2C.

90. For an incisive and comprehensive analysis of a similar hypothetical, see Harvey Wingo, *A 2020 Vision of Visual Surveillance and the Fourth Amendment*, 71 OR. L. REV. 1 (1992).

91. In developing their own analyses, for example, Professor Power and Professor Steinberg make no mention of many of these factors. Professor Power appears to focus primarily on factors (1) (location), (5) (availability) and (7) (minimization). *See* Power, *supra* note 79, at 87-111. Professor Steinberg's analysis consists of three components: one analogous to factor (3) (nature of target) and two related to factor (7), which are balanced to determine whether a warrant is required. *See* Steinberg, *supra* note 80, at 613 (arguing that the specificity of the information revealed, the duration of the search, and the extent to which the enhanced search requires officers to focus on a particular individual are the key variables).

many important issues unresolved. These unresolved issues can be divided into four categories: implementation of authorized surveillance, selection of rulemakers, selection of decisionmakers, and accountability.

The two most important implementation issues that have yet to be comprehensively addressed concern the *results* of physical surveillance. Consider, for instance, the fact that video surveillance of public areas can produce hours of tape that might be useful for any number of purposes: from identifying perpetrators of violent crime to identifying jaywalkers; from recording speeders to recording traffic accidents; from discovering which people visit a certain area to discovering whether an alleged adulterer visits his alleged paramour. The first issue raised by this reality concerns disclosure. To whom and for what purposes may such tapes be disclosed? The second issue pertains to retention. For how long and for what purposes may such recordings be maintained? Current law is almost silent as to whether information obtained for one purpose may be used for another, or when recordings of an investigation should be destroyed.[92]

Several other implementation issues are also left unaddressed by case law and legislation. One interesting question is whether the subjects of completed covert physical surveillance are entitled to notice of the surveillance. Another is whether police should have to validate the reliability of the technology they use.

The second set of unresolved issues concerns the entities that construct the rules regulating physical surveillance. Courts will probably be the primary players when the Constitution is implicated.[93] But implementation of broad constitutional mandates often requires fine tuning.[94] Furthermore, physical surveillance that is *not* restricted by constitutional precepts might nonetheless justifiably be subject to some limitation.[95] By imposing rules when constitutional interpretation is not involved, courts might be usurping others' authority — legislatures,

---

92. *Cf.* Britt v. Naval Investigative Serv., 886 F.2d 544, 550 (3d Cir. 1989) (holding that the Privacy Act, 5 U.S.C. § 552(a) (1996), may bar disclosure of information obtained by the Naval Investigative Service to the subject's employer, the Immigration and Naturalization Service, at least when no charges are filed); Covert v. Harrington, 876 F.2d 751, 755 (9th Cir. 1989) (suggesting that collecting information for security-clearance purposes might be incompatible with disclosing it for criminal investigation purposes).

93. *But see* Craig M. Bradley, *Criminal Procedure in the "Land of Oz": Lessons for America*, 81 J. CRIM. L. & CRIMINOLOGY 99, 131-32 (1990) (arguing that Congress has the authority, under section 5 of the Fourteenth Amendment, to pass a code of criminal procedure based on constitutional precepts).

94. For instance, the FBI has developed informal guidelines on the use of beepers. Personal Communication with Scott Charney, Chief, Computer Crime Unit, U.S. Department of Justice (Feb. 10, 1997).

95. *See infra* text accompanying notes 123-27, 187-88.

municipal bodies, and the police themselves could serve as rulemakers in both situations.[96]

Regarding who should decide whether an established rule authorizes a particular surveillance action, Fourth Amendment case law recognizes numerous situations where a police officer, rather than a judge, is the appropriate arbiter.[97] It fails to recognize, however, that other entities could be consulted as well. Especially in non-exigent circumstances that do not implicate the Fourth Amendment, legislative bodies, prosecutors, and the public affected by the surveillance might all be involved in the decisionmaking process. Further, when the police are delegated decisionmaking responsibility, distinctions might be made between different levels of decisionmakers (e.g., field officers versus supervisors).

Accountability is the final important physical surveillance issue only partially addressed by the case law. Courts, lacking any direct control over law enforcement agencies and other government officials, have relied primarily on exclusionary rules as an enforcement mechanism.[98] But this sanction has been controversial, to put it mildly.[99] Accordingly, the rule is often not invoked even when a constitutional violation has occurred,[100] much less when a subconstitutional rule is involved. In the latter situations, other types of sanctions might be advisable; indeed, even when exclusion is appropriate additional sanctions might be

---

96. A significant body of literature recognizes the possibility that these entities can and even should play a role in rulemaking. *See, e.g.*, Amsterdam, *supra* note 79, at 423-29 (enumerating the reasons police should be involved in rulemaking); STANDARDS FOR CRIMINAL JUSTICE § 1-4.3 (2d ed. 1980 & Supp. 1986) ("Police discretion can best be structured and controlled through the process of administrative rule making by police agencies. Police administrators should, therefore, give the highest priority to the formulation of administrative rules governing the exercise of discretion, particularly in the areas of selective enforcement, investigative techniques, and enforcement methods."); Samuel Walker, *Controlling the Cops: A Legislative Approach to Police Rulemaking*, 63 U. DET. L. REV. 361, 363-64, 382-84 (1986) (arguing that legislation is necessary to guide police rulemaking); JAMES Q. WILSON, VARIETIES OF POLICE BEHAVIOR 284-90 (1968) (discussing ways in which the community could be involved in rulemaking).

97. For a list of "exigent circumstances" in which field officers may make warrantless searches, see CHARLES H. WHITEBREAD & CHRISTOPHER SLOBOGIN, CRIMINAL PROCEDURE 132-33 (3d ed. 1993).

98. *See* Mapp v. Ohio, 367 U.S. 643, 652 (1961) (holding that evidence seized in violation of the Fourth Amendment should be excluded, in part because other remedies are "futile").

99. *See generally* Office of Legal Policy, U.S. Department of Justice, *Report to the Attorney General on the Search and Seizure Exclusionary Rule*, 22 U. MICH. J.L. REFORM 573, 608-617 (1989) (detailing the costs of the exclusionary rule, including a failure to deter police, lost convictions, disrespect for the judicial system, failure to provide a remedy for the innocent, and the insidious effect on probable cause determinations by judges).

100. *See* United States v. Leon, 468 U.S. 897, 923-24 (1984) (holding that exclusion is not required even when the Fourth Amendment is violated if evidence is seized in good faith reliance on a warrant).

imposed. If so, as with rulemaking and decisionmaking, legislative and administrative entities might be involved in ensuring accountability for violations of the rules. Moreover, accountability need not be solely a matter of sanctions. Documentation of surveillance decisions, periodic review of those decisions, and public dissemination of information about physical surveillance might also make the police feel accountable for the surveillance they conduct.[101]

It is quite understandable why, given their limited role, courts have not dealt with these types of implementation, rulemaking and decisionmaking, and accountability issues. Many of these issues are not, and probably should not be, accorded constitutional status; that does not make them unworthy of consideration, however. Any attempt to regulate law enforcement use of physical surveillance comprehensively must at least consider the various options that are available.

III. THE ABA'S APPROACH: AN OVERVIEW

The regulatory principles that can be derived from the case law governing physical surveillance are inadequate in a number of ways. Legislation has yet to fill the legal void. The Task Force's Draft Standards attempt to rectify this situation by providing guidelines for policymakers, judges, and police departments.

The Task Force's efforts proceeded through three conceptual stages. The first stage consisted of identifying the scope of the problem. The second stage involved the development of general principles that should govern the use of physical surveillance technology. The final stage involved elaboration of these general principles in specific contexts.

A. The Categories of Technologically-Assisted Physical Surveillance

In addition to learning the relevant law, an initial goal of the Task Force was to determine the types of physical surveillance devices that are or may become available to the police. The Task Force heard expert briefings on this topic from the Federal Bureau of Investigation, the Science and Technology division of the National Institute of Justice, the Director of Community-Oriented Policing Services at the Department of

---

101. The Electronic Surveillance Standards require annual reports from both judges and prosecutors concerning the number of surveillance orders applied for, denied and granted, the duration of the surveillance, the identity of those authorizing and executing the surveillance, and a number of other facts relating to surveillance orders. *See* Electronic Surveillance Standards, *supra* note 7, Standard 5.16. They also require that information from the reports be disseminated to the public. *See id.* Title III requires public dissemination of similar information. *See* 18 U.S.C. § 2519 (1994).

Justice, and two state police representatives. In addition, the Task Force sought comments on an earlier version of the Draft Standards from eight police organizations, ranging from the International Association of Chiefs of Police to the National Sheriffs Association.[102]

As a result of this input and its own investigations, the Task Force divided physical surveillance devices into five separate categories:[103] video cameras, tracking devices, telescopic devices, illumination devices, and detection devices (i.e., devices capable of detecting concealed items).[104] These functional groupings are meant to describe the spectrum of physical surveillance technologies that exist at present and that might be developed in the foreseeable future. Only time will tell whether they are adequate in the latter regard.

Video technology has been available for some time, but the past three decades have seen dramatic advances in the field. With the advent of wide-angle and pinhole lenses, night vision equipment, and super-magnification capability, video surveillance allows viewing of home interiors, workplaces, and public thoroughfares at all times. Cameras can be placed in picture frames, briefcases, pens, suit lapels, and teddy bears, permitting covert observation in virtually any circumstance.[105] They also can be used overtly and conspicuously to observe private establishments

---

102. The Task Force sought comments from the Fraternal Order of Police, the International Association of Chiefs of Police, the International Union of Police Organizations, the Major Cities Chiefs, the National Association of Police Organizations, the National Sheriffs Association, the Police Executive Research Forum, and the U.S. Department of Justice (Community Oriented Police Services).

103. This division was based largely on a memorandum from Wayne LaFave to the Task Force (July 27, 1995) (on file with the *Harvard Journal of Law and Technology*).

104. Originally, and for almost the full two years of the Task Force's work on the physical surveillance standards, a sixth category also existed – aerial surveillance. This category was ultimately dropped for two reasons. First, to the extent aerial surveillance makes use of enhancement devices (e.g., map-making cameras), the other specific rules already govern. Second, aircraft are functionally no different from cars, boats and other vehicles; they assist the use of investigative technology but are not themselves devised for the purpose of surveillance. Despite the deletion of this category, however, case law governing aerial surveillance played a significant role in shaping the Task Force's thinking. *See supra* Part II.A.

105. *See, e.g.*, Thompson v. Johnson County Community College, 930 F. Supp. 501, 506 (D. Kan. 1996) (upholding video monitoring of security personnel locker area); James Barron, *Designer/Surveillance Consultant Sells Pricey Spy Ties*, SAN ANTONIO EXPRESS-NEWS, Sept. 22, 1996, *available in* 1996 WL 11498094 (describing various items, including ties and teddy bears, into which video cameras can be installed); Kim Christensen, *Snoopy Sales//Spies: Don't Look Now, But Big Brother Might Just Be Your Big Brother*, ORANGE COUNTY REG., Aug. 2, 1996, *available in* 1996 WL 7041469 (explaining the use of pinhole-lens video cameras in briefcases and wall clocks).

and public places.[106] Furthermore, any surveillance by camera can be recorded, creating a permanent record of activities within the camera's range.[107]

Tracking devices also come in many forms. The simplest is the beeper, which emits a signal that can be traced.[108] Other tracking devices under development or already in use include "over-the-horizon" radar;[109] bistatic sensor devices, which passively pick up various types of emissions (e.g., from a cellular phone or a light source) or utilize an active sonar-like capability;[110] and tagging systems, which use a projectile launcher to attach a beeper to a fleeing vehicle.[111] Intelligent Transportation Systems (sometimes called Intelligent Vehicle Highway Systems) involve fitting every vehicle in a given transportation network with a radio unit that transmits to a base station.[112] While being studied principally as a means of controlling traffic patterns, these systems would also provide a way of tracking vehicles, or of discovering their location at a previous point in time.[113]

Unlike modern video surveillance and tracking systems, some types of telescopic and illumination devices — binoculars and telescopes, flashlights and spotlights — have been available for more than a century.

---

106. David Kocieniewski, *Police to Press Property-Crime Fight and Install Cameras*, N.Y. TIMES, Feb. 5, 1997, at B4 (reporting that the New York City Police Department will install new video surveillance cameras in some housing projects and subway stations).

107. Of course, video surveillance can be accompanied by audio capabilities as well, a practice governed by the Electronic Surveillance Standards, *supra* note 7.

108. *See* Note, *Tracking* Katz*: Beepers, Privacy and the Fourth Amendment*, 86 YALE L.J. 1461, 1463-64 (1977) (explaining that beepers emit "periodic signals which can be picked up on radio frequency [to] establish the approximate location of the object .... Beepers have been used ... to trace the movement of subjects on private property, along public thoroughfares, or in public airways ... [and] have [been] attached ... to contraband drugs discovered during border searches, to motor vehicles used by suspects, to packages or drums of chemicals, to airplanes, and to an item of personal property").

109. *See* Department of the Air Force, Rome Laboratory, Over-the-Horizon Radar, Advanced Technology Data Sheet (abstract presented at National Institute of Justice Law Enforcement Technology Program, May 15, 1995) (on file with the *Harvard Journal of Law and Technology*).

110. *See* Department of the Air Force, Rome Laboratory, Electronic Support Measurement, Bistatic Sensor Technology, Advanced Technology Data Sheet (abstract presented at National Institute of Justice Law Enforcement Technology Program, May 15, 1995) (on file with the *Harvard Journal of Law and Technology*).

111. *See* Idaho Nat'l Engineering Laboratory, Fleeing Vehicle Tagging System (abstract presented at National Institute of Justice Law Enforcement Technology Program, May 15, 1995) (on file with the *Harvard Journal of Law and Technology*).

112. *See* U.S. DEP'T OF TRANSP., NATIONAL PROGRAM PLAN FOR INTELLIGENT TRANSPORTATION SYSTEMS (Final Draft 1994) (on file with the *Harvard Journal of Law and Technology*).

113. *See* Jeffrey H. Reiman, *Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future*, 11 SANTA CLARA COMPUTER & HIGH TECH. L.J. 27 (1995).

Today, however, new technology provides would-be viewers with significantly greater ability to overcome obstacles created by distance and darkness. Compact night-vision equipment using infrared technology enables covert observation of virtually any nighttime activity,[114] while map-making and satellite cameras are able to focus on objects a few feet across from thousands of feet above.[115] Moreover, illumination and telescopic capabilities can be combined in one instrument, as with the well-known Startron binoculars.[116]

Detection systems include a wide range of devices using x-ray, heat sensing, holographic radar, and other technologies. Simple metal detectors will soon be augmented with hand-held devices that can discern the shape and size of items underneath a person's clothing, or even behind walls; some of these devices may also reveal anatomical details.[117] One such tool, developed by Millitech Corporation, registers radiation emitted from the body and objects concealed on it.[118] Because these waves readily pass through clothing, and because the body is a good emitter while dense, inanimate objects tend to be bad emitters, inanimate objects show up as outlines against the body. A device developed by Raytheon aims a low-intensity electromagnetic pulse at the subject and measures the time-decay of each object radiated, which differs depending upon the object. The device then compares the time-decay of each object with known "signatures" of items like guns; no image is produced.[119] A third example, from INEL, measures the fluctuations in the earth's magnetic field caused by ferromagnetic material, like the metal in a gun.[120] Other mechanisms have been

---

114. For instance, infrared technology used in ITT's Night Enforcer allows night vision in low-light conditions without any illumination that would give the observer away. These devices are held in one hand, obtain high resolution, offer photo and telescopic capability, and prevent "blooming" when bright light sources are encountered. *See* ITT Electro Optics Product Division, Night Enforcer 250, ITT Night Vision Equipment (abstract presented at National Institute of Justice Law Enforcement Technology Program, May 15, 1995) (on file with the *Harvard Journal of Law and Technology*). For a general description of many of these devices, see Gutterman, *supra* note 83, at 678.

115. For a description of some of the telescopic equipment in use today, see *supra* note 89. With respect to satellite surveillance, see Kelly, *supra* note 2, at 737 (describing current ability "to generate and sell images derived from satellites capable of detecting objects as small as one square yard").

116. *See* Cook, *supra* note 89.

117. *See* Millitech Corp., Millimeter Wave Concealed Weapon Detection and Through-the-Wall Imaging Systems (abstract presented at National Institute of Justice Law Enforcement Technology Program, May 15, 1995) (on file with the *Harvard Journal of Law and Technology*).

118. *See id.*

119. *See* David A. Harris, *Superman's X-Ray Vision and the Fourth Amendment: The New Gun Detection Technology*, 69 TEMPLE L. REV. 1, 7-8 n.38 (1996).

120. *See id.*

developed for detecting hidden explosives[121] and heat differentials from a building (which might signal the use of kleig lights or furnaces connected with the growth or manufacture of contraband).[122]

B. The General Principles

Having provisionally defined the types of physical surveillance subject to regulation, the Task Force set out to develop overarching principles to guide that regulation. The result is Standard 2-6.1, the "general principles" standard. This Standard consists of seven sections, which are only briefly outlined here. Detailed discussion of some of the more controversial provisions is found in Part IV.

The first two sections of Standard 2-6.1 set the conceptual stage for the rest of the Standards by specifying the various interests that are implicated by law enforcement use of technologically-assisted physical surveillance. Section (a) identifies the ways in which such surveillance might be useful to law enforcement, while section (b) identifies the societal harms it might cause.

More specifically, section (a) recognizes that technologically-assisted physical surveillance might further many legitimate law enforcement ends, from the detection, investigation, and deterrence of crime to the protection of the innocent. Moreover, technology might prove more reliable, less expensive, safer, and less intrusive than traditional means of conducting surveillance. For instance, a permanent video camera might be able to identify perpetrators more accurately and at less expense than police patrols. Beepers can track a target for prolonged periods, saving human capital and decreasing physical danger. Weapon-detection devices might permit discovery of concealed weapons from a distance with greater accuracy and less danger to the police than a frisk, and with less inconvenience and embarrassment to the target.

At the same time, as section (b) recognizes, the use of these devices "can diminish privacy, freedom of speech, association and travel, and the openness of society." Physical surveillance of the home and similar locations obviously poses significant risks of privacy invasion. But even physical surveillance of more open areas can threaten values considered important in a democratic society. Alan Westin, for example, has theorized that the privacy concept encompasses four "states": solitude,

---

121. *See* Golden Engineering, XR150 (information presented at National Institute of Justice Law Enforcement Technology Program, May 15, 1995) (on file with the *Harvard Journal of Law and Technology*).

122. Such devices are sometimes called FLIRs (Forward Looking Infrared). *See generally* Scott J. Smith, *Thermal Surveillance and the Extraordinary Device Exception: Redefining the Scope of the* Katz *Analysis*, 30 VAL. U. L. REV. 1071 (1996).

intimacy, anonymity, and repose.[123] Because people occasionally seek these four states even in public spaces, privacy might be diminished by virtually any type of public surveillance — including observation by simple binoculars. Technologically-assisted physical surveillance can diminish other values as well. For instance, freedom of speech and association can be chilled through conspicuous video or telescopic surveillance, as Orwell's *1984*[124] vividly demonstrates. The right to travel might be infringed by the constant monitoring allowed by Intelligent Transportation Systems. Most generally, the openness of society, a quality arguably essential to a well-functioning democracy,[125] might be threatened by pervasive monitoring.

To aid in deciding when, and to what extent, *particular* surveillance should be regulated, section (c) of the general principles elaborates on the competing factors outlined in sections (a) and (b). On the law enforcement side, the nature of the law enforcement objective, the extent to which it can be achieved through surveillance, and the seriousness of the crime problem being investigated, deterred, or protected against are all relevant in determining whether surveillance is justified. With respect to privacy and related interests, section (c) lists the seven factors drawn from the case law identified earlier[126] and adds three more: whether the surveillance is covert or overt; the extent to which the surveillance diminishes or enhances First Amendment freedoms; and the extent to which "the surveillance technique is less intrusive than other available effective and efficient alternatives." Thus, for instance, airport surveillance using video cameras and detection devices might be more easily justified than ordinary investigative surveillance using this technology because of the significant interest in deterring terrorism, the overt nature of such surveillance, and the fact that other methods are more intrusive

---

123. WESTIN, *supra* note 1, at 31-32.

124. GEORGE ORWELL, 1984 (Bernard Crick ed., Oxford University Press 1984) (1949).

125. Totalitarian regimes maintain power not through the consent of the governed but by physical, economic, and psychological control over the populace. Such governments exercise control through a variety of means, but among the most essential is the use of the police power to reinforce the message that the government is superior and in control of the individual. Measures such as identification checkpoints, random searches, the monitoring of communications, and the widespread use of informants not only are means of keeping track of the citizenry, but also act as continuous symbolic reminders that the citizenry is dominated by the government.

Scott Sundby, *"Everyman"'s Fourth Amendment: Privacy or Mutual Trust Between Government and Citizen*, 94 COLUM. L. REV. 1751, 1778-79 (1994).

126. *See supra* Part II.A.

or less efficient. Other examples of this balancing analysis are discussed below.[127]

Surveillance that is duly authorized is still illegitimate if it is not carried out properly. Section (d) of the general principles lists restrictions on the manner in which surveillance should be conducted. These include rules dealing with the scope of the surveillance, the types of devices used, notice to those observed, and disclosure and maintenance of surveillance records.

First, to avoid discrimination, section (d) provides that subjects of surveillance should not be selected in an arbitrary manner; this admonition is especially important where individualized suspicion might not be required, as with checkpoints.[128] Second, for obvious reasons, "[t]he scope of the surveillance should be limited to its authorized objectives and be terminated when those objectives are achieved."[129] Because new surveillance techniques, some of doubtful efficacy,[130] are continuously entering the market, the third subsection of this provision cautions that the physical surveillance technology used "should be capable of doing what it purports to do and be used solely by officers trained in its use." Fourth, to address situations in which a device might simultaneously make use of more than one technology covered by the specific standards (e.g., a video camera with telescopic and illumination capabilities), section (d) also states that, where there is a conflict between rules, the more restrictive one applies.[131]

The fifth provision in section (d) states that "[r]easonable notice of the surveillance should be given at an appropriate time and in an

---

127. *See infra* Part III.C.

128. *Cf.* Delaware v. Prouse, 440 U.S. 648 (1979) (holding that suspicionless, random stops of cars to check licenses violate the Fourth Amendment).

129. The appropriate conduct when the surveillance does not achieve its objective within a certain period of time is unclear under the standard. On this issue, the preliminary commentary states: "Certainly some [types of procedures] should have fixed time limits, at least absent an extension granted by the authorizing person or agency. In some instances, it may suffice that the surveilling officers are required to determine for the record why they find the surveillance sufficiently promising to continue it." TENTATIVE DRAFT STANDARDS CONCERNING TECHNOLOGICALLY-ASSISTED PHYSICAL SURVEILLANCE § 2-6.1(d)(ii) commentary (Draft, Feb. 20, 1997) (on file with the *Harvard Journal of Law and Technology*).

130. *See, e.g.*, Erik Milstone, *Improbable Cause: Prosecutors Say Police May Have Made Arrests Based on Questionable "Narcotics Divining Rod"*, 82-JUN A.B.A. J. 32 (1996) (reporting that the Quadro Tracker, a $3,000 drug detection device with sales of over 1,000, "is little more than a black plastic box with a radio antenna attached to one end that swirls when the box is moved," according to the Sandia National Laboratories).

131. For example, although cursory, overt use of an illumination device might not require any justification, *see* Standard 2-6.5(b)(i), *infra* Appendix, if the device had a video capability it would require a supervisor's finding that the legitimate law enforcement test had been met, *see* Standard 2-6.3(c), *infra* Appendix.

effective manner." In some situations (e.g., checkpoints), pre-surveillance notice may be necessary to maximize deterrence and prevent public alarm.[132] In others, post-surveillance notice to those subjected to the surveillance may be advisable or even constitutionally required.[133]

The final provisions of section (d) also involve post-surveillance issues. By permitting disclosure of surveillance results only for "designated" lawful purposes, provision (d)(vi) attempts to encourage law enforcement officials, legislatures, and courts to adopt a regime that relies on rules specifying when and to whom surveillance results may be disclosed. The same design lies behind provision (d)(vii) requiring "protocols" for the maintenance and disposition of surveillance records.

The primary objective of section (e) of the general principles is to emphasize that courts are not the sole source of law, nor are magistrates and police officers the sole implementers of that law. To that end, the section lists various entities that might be involved in formulating, monitoring, and enforcing the regulation of technologically-assisted physical surveillance, and identifies factors that can help determine when each entity might best be involved.

The first such factor is the "legal basis" of the proposed rule. If surveillance implicates the Fourth Amendment, courts are likely to be the source of rules and sanctions, although legislatures and administrative agencies might attempt to codify the rules developed.[134] In other situations, whether the legislature, law enforcement officials, or the public should be involved depends upon the "invasiveness and urgency of the surveillance," the "need for deference to expertise in law enforcement," the "extent to which local conditions may vary," the "value of sharing decisionmaking," and the "number of people and size of the geographic area affected by the surveillance."

This general principle departs somewhat from the standard Fourth Amendment model in which courts make the law and either magistrates (in non-exigent situations) or field officers (in exigent circumstances) apply it. For example, given the number of people affected, the primary rules governing placement of public video cameras or detection-device checkpoints might come from municipal or state legislatures as well as courts. Because local crime conditions vary and police have knowledge

---

132. *Cf.* United States v. Martinez-Fuerte, 428 U.S. 543, 559 (1976) (upholding checkpoint preceded by signs announcing its presence, in part because "[m]otorists using these highways are not taken by surprise as they know, or may obtain knowledge of, the location of the checkpoints and will not be stopped elsewhere.").

133. *See* Berger v. New York, 388 U.S. 41, 60 (1967) (holding a New York wiretapping statute unconstitutional because, *inter alia*, it "has no requirement for notice as do conventional warrants, nor does it overcome this defect by requiring some showing of special facts").

134. *See supra* text accompanying notes 93-97.

of those conditions, more specific rules concerning such surveillance might be developed by individual police departments (a position emphasized in section (g), discussed below). Further, section (e) suggests that in determining where any *particular* camera or checkpoint should be situated, *neither* a judge *nor* a field officer should be involved. Rather, to ensure that decisions are based on all relevant information and will be accepted by those affected, those decisions might involve politically accountable police or local governmental officials, as well as the public to be targeted by the surveillance.[135] Similarly, the emphasis on the value of shared decisionmaking suggests that, in non-exigent circumstances not governed by the Fourth Amendment, a police *supervisor* should be involved in the surveillance decision.[136]

Section (f) of the general principles focuses on the accountability of those conducting surveillance. Ensuring accountability is especially important in this context because so much technologically-assisted physical surveillance is covert and thus does not alert its targets the way a typical search and seizure does. The standard recognizes that the exclusionary rule is required in some situations, but adds a number of other accountability mechanisms. First, it provides that government officials should develop "administrative rules which ensure that the information necessary for . . . accountability is maintained." Second, it calls for administrative sanctions for violation of surveillance rules, in addition to any constitutionally required exclusionary sanctions. Periodic review of the scope and effectiveness of surveillance is also mandated. Finally, similar to the reporting requirements under the federal wiretapping statute,[137] the standard provides that "information about the general type or types of surveillance being used and the frequency of their use" should be disseminated to the public in an effort to keep the polity apprised of the extent of surveillance being conducted.

Section (g), the final provision in the general principles standard, calls for administrative rulemaking by law enforcement officials. Especially as to limitations that are not constitutionally required and that consequently never receive attention from courts or magistrates, a

---

135. This position is taken in the standards governing long-term public video surveillance and checkpoints using detection devices. *See* Standards 2-6.3(b)(ii) & 2-6.6(a)(iv)(D), *infra* Appendix.

136. *See* Standard 2-6.3(b) & (c), *infra* Appendix (requiring approval from a politically accountable official for long-term video surveillance of nonprivate activities, locations, and conditions and approval from a supervisor for other video surveillance of nonprivate activities, locations and conditions); Standard 2-6.6(a)(iv), *infra* Appendix (requiring approval from a politically accountable official for fixed checkpoints and from a supervisor for temporary checkpoints).

137. *See* 18 U.S.C. § 2519 (1994) (requiring annual reports concerning frequency of intercepted wire, oral, or electronic communications).

particular need for elaboration within the administrative process exists; individual officers cannot be expected to work everything out for themselves in these situations. Thus section (g) proposes that departments should develop policies that translate the general principles and the specific rules of the standards into detailed guidelines for various forms of physical surveillance.

Again, the purpose of the general principles is to provide a framework for analyzing regulatory issues raised by physical surveillance. Some of the principles were used in developing more specific rules. For instance, section (c), concerning when surveillance is justified, dictates whether probable cause or some lower level of certainty is required before surveillance can take place. Similarly, section (e), dealing with the decisionmaker, controls when field officers, higher level officials, and the public are involved in decisionmaking. In contrast, the principles described in section (d), concerning implementation of the surveillance, and section (f), concerning accountability, were meant to stand on their own without further elaboration in the specific standards. They were not repeated in each of the specific standards because they usually apply in the same fashion to any surveillance.

C. Definitions

Standard 2-6.2 contains ten definitions. Half of these definitions explain the types of enhancement devices governed by the standards — detection devices, illumination devices, telescopic devices, tracking devices, and video surveillance. Other terms defined are "covert" and "overt" surveillance, "reviewing law enforcement official," "private," and "legitimate law enforcement objective."

Although the various devices have already been described, the definition of detection devices in section (b) requires some elaboration. This term is defined to include any device that detects "the presence of a particular object . . . or characteristic . . . that is concealed behind opaque inanimate barriers." Devices that detect microscopic substances or that "see" through human bodies are not covered by this definition. On the other hand, devices that can "see" through clothing, wood, metal, or other substances are included.[138]

A further distinction is made between general detection devices and those that are "contraband-specific" and "weapon-specific." Although most detection devices (e.g., x-ray machines and magnetometers currently used at airports) are of the former variety, some devices purport to detect only guns or explosives,[139] and someday devices may simulate

138. *See supra* text accompanying notes 117-22.
139. *See supra* notes 119 & 121.

the capability of "drug dogs" by signaling only the presence of contraband.

The general-specific distinction is important in light of case law indicating that the Fourth Amendment is not implicated by a police action that detects only contraband.[140] As this section recognizes, whether an object is "contraband" will depend upon whether the item is "virtually always criminal to possess or use in the existing circumstances." Carrying drugs like marijuana or cocaine is virtually always criminal. Carrying a concealed weapon, on the other hand, is not. Possessing a weapon is virtually always criminal at an airport, but in the majority of states today, carrying a concealed weapon is legally permissible.[141] In such states, a device that detected only guns would not be a contraband-specific device under this definition, although it would be a weapon-specific device.

Video surveillance, as defined in section (j), also requires elaboration. It is defined to exclude use of a "lawfully positioned" camera to view or record activities "occurring within the sight or immediate vicinity of a law enforcement official (or agent thereof) who is aware of such use."[142] For example, cameras in police cruisers or on uniform lapels would not be video surveillance for purposes of the standards. On the other hand, the camera must be lawfully positioned. Thus, the use of a camera to view what an undercover agent can see, while normally not encompassed by this definition, constitutes video surveillance if the camera has been illegally installed in a house.

The distinction between covert surveillance and overt surveillance is important for several reasons. Under these standards, post-surveillance notice is not required for overt surveillance, whereas it may be required for certain types of covert surveillance.[143] Also, covert video surveillance of nonprivate places is not regulated as strictly as long-term

---

140. *See* United States v. Jacobsen, 466 U.S. 109, 123 (1984) (holding that a field test to reveal whether a substance is cocaine is not a search); United States v. Place, 462 U.S. 696, 707 (1983) (holding that a canine sniff is not a search).

141. *See* Michael Janofsky, *Thousands Seek Permits to Carry Concealed Arms*, N.Y. TIMES, July 6, 1995, at A14 (reporting that twenty-five states have laws that allow "almost all" adults to carry concealed firearms, while other states require a showing of "special need").

142. This definition is consistent with Supreme Court case law holding that one assumes the risk that people with whom one converses are electronically recording the conversation. *See* On Lee v. United States, 343 U.S. 747 (1952) (holding that a microphone carried by an informant does not violate the Fourth Amendment); United States v. White, 401 U.S. 745 (1971) (holding that risk of a companion reporting to the police is not altered by the use of electronic equipment).

143. *See* Standard 2-6.1(d)(v), *infra* Appendix.

overt video surveillance.[144] Finally, brief overt use of telescopic and illumination devices to view nonprivate activities is not regulated at all, while covert use of these technologies is.[145]

The definitions in sections (a) and (e) resolve close cases in favor of finding the surveillance to be covert. Consider the use of binoculars from a police car. One might say such use is overt if there is no attempt to hide from passersby. However, under this definition, it is covert if the officer intends that the subject of the surveillance be unaware of the monitoring and if a reasonable person in the subject's position would be unaware of it.

The definition of "reviewing law enforcement official" in section (g) implements the call of general principle 2-6.1(e) for administrative involvement by recognizing multiple levels of decisionmaking authority. At a minimum, this definition indicates, there are three such levels: the observing, or field, officer; an immediate supervisor (perhaps a sergeant or captain); and the head of the department, who will normally be politically accountable either through the election or appointment process. Given the diversity of command structures,[146] it would be unwise to attempt any more specificity.

Nevertheless, the three basic distinctions are crucial to the standards' approach to decisionmaking. Generally speaking, under the standards the field officer is authorized to make decisions about using physical surveillance technology only when exigent circumstances exist or the intrusion involved is minor.[147] A high-level department official or a police supervisor is the authorized decisionmaker in all other situations

---

144. *Compare* Standard 2-6.3(c), *infra* Appendix (covert surveillance) *with* Standard 2-6.3(b), *infra* Appendix (long-term overt surveillance).

145. *Compare* Standard 2-6.5(b)(i), *infra* Appendix (overt, cursory use of illumination and telescopic devices) *with* Standard 2-6.5(b)(ii), *infra* Appendix (covert use of such devices).

146. Police organizations can range from a sheriff's office with one or two deputies to a huge, military-type operation with ranks ranging from patrol officer through sergeant, lieutenant, captain and chief. *See generally* ROBERT H. LANGWORTHY, THE STRUCTURE OF POLICE ORGANIZATIONS (2d ed. 1986).

147. In non-exigent circumstances the field officer may, without supervision: (1) install and monitor tracking devices so long as no entry into a private place is required for installation, and monitoring of the device does not disclose the contents of a private place, *see* Standard 2-6.4(a) - (b), *infra* Appendix; (2) use illumination and telescopic devices to observe nonprivate places, *see* Standard 2-6.5(b), *infra* Appendix; (3) use detection devices whenever a warrantless search is permitted by the Fourth Amendment, *see* Standard 2-6.6(a)(I)-(iii), *infra* Appendix, whenever the device is contraband-specific and is not used to observe a private residence, *see* Standard 2-6.6(b), *infra* Appendix, or whenever the device is weapon-specific and is used in situations that predicate a weapons search, *see* Standard 2-6.6(c), *infra* Appendix.

in which the Fourth Amendment does not require a judge to be involved.[148]

Two final definitions are particularly important to understanding the regulatory scheme adopted by the standards. The first is the definition of "private" in section (f), which simply consists of a cross-reference to case law and to the factors listed in general principle 2-6.1(c)(ii). This definition is designed to indicate which situations implicate the Fourth Amendment, and thus trigger either the warrant and probable cause requirements or, in the case of checkpoints, other special protections.[149] While amorphous, the definition does at least identify the universe of variables that might be considered in making this elusive determination. Furthermore, the second sentence of this definition states that, where the standards refer to a *place*, the area is "private" if physical entry into it would be considered a Fourth Amendment search. Thus, when the phrase "private place" is used (in connection with tracking and detection devices[150]), Fourth Amendment protection extends to houses, luggage, and similar items regardless of whether steps have been taken to ensure privacy or the other considerations found in Standard 2-6.1(c)(ii).

The definition of "legitimate law enforcement objective" in section (d) is closely connected to the definition of "private." Throughout the standards, the propriety of surveilling a *nonprivate* area, activity, or condition depends on whether the surveillance is "reasonably likely to achieve a legitimate law enforcement objective."[151] In other words, this phrase provides the standard that police must meet in those situations not governed by the Fourth Amendment. For obvious reasons, these situations have received little attention from the courts.[152] Thus, the language of Standard 2-6.2(d) introduces a new regulatory concept.

This concept has two essential elements. First, it incorporates the general principle in Standard 2-6.1(a) that all surveillance should be for an investigatory, deterrent, preventive, or protective purpose.[153]

---

148. *See supra* note 136.

149. *See* Standard 2-6.6(a)(iv), *infra* Appendix.

150. *See* Standards 2-6.4(a) & 2-6.6, *infra* Appendix.

151. *See, e.g.*, Standard 2-6.3(c), *infra* Appendix (covert video surveillance) and Standard 2-6.4(b), *infra* Appendix (monitoring of a tracking device).

152. *But see* Sitz, 496 U.S. at 453 (permitting sobriety checkpoints that are "reasonable alternatives" to other means of deterrence); Griffin v. Wisconsin, 483 U.S. 868, 878 (1987) (holding that searches of probationers' homes need not be based on probable cause but rather could occur under a statute requiring only "reasonable grounds").

153. Typically, these purposes relate to criminal activity. However, there may be some situations when surveillance can legitimately be used to prevent harm not associated with crime. For instance, an officer monitoring a video camera panning a public street might observe a pedestrian bend over in an ambiguous but disconcerting manner; certainly the use of a zoom capability to see if the person is in distress is legitimate in this situation.

Surveillance for ends that are purely political, or for the purpose of harassment, does not pursue a legitimate law enforcement purpose.[154]

The second essential element is the "reasonably likely" criterion. As defined in section (d), this language requires "articulable reasons" for concluding that, through the surveillance, an offense will be discovered, come closer to being solved, or be deterred, or a harm will be prevented. At first glance, this definition may look like the reasonable suspicion standard defined in *Terry v. Ohio*,[155] which requires "specific and articulable" facts as the basis for a stop or frisk.[156] Note, however, that what is required here is not a finding that a particular person will be tied to a particular crime (which is individualized suspicion), but rather articulable reasons that the surveillance will further investigative, deterrent, or protective ends.

Suppose, for instance, that police want to videotape the people who go into a suspected crack house. They are likely to have little or no suspicion with respect to any given individual who is observed, but they may well have an articulable reason for believing the videotape will help accomplish an investigatory end if covert, or a deterrent end if overt. Or suppose police want to use binoculars to observe, without being discovered, an area known for dangerous drug trafficking. There may be no suspicion with respect to any particular person observed, but there may be an articulable reason for concluding that useful information will be obtained or that the protection of officers who enter the area will be enhanced.

Although it thus does not require as much of a showing as reasonable suspicion, the "reasonably likely" language requires that the police articulate their objectives. Generally speaking, it was the intent of the Task Force that investigative objectives should be driven by a *particular* offense or type of offense, rather than a generalized concern about crime, and that deterrence objectives be associated with a *significant*, demonstrable crime problem. Without these limitations, all police surveillance could be said to have an articulable basis, since regardless of the location or time, there is always a slim possibility that some sort of crime or event of future evidentiary significance will occur.

Thus, while the phrase "reasonably likely" may permit video surveillance of the public space in front of a federal building, it does not permit surveillance of a public park simply to have a record of who was

---

154. *See* WESTIN, *supra* note 1, at 128-29 (describing the use of surveillance to extract pay off money, learn the plans of opposing politicians, monitor political protest groups, and eavesdrop on attorney-client conversations).

155. 392 U.S. 1 (1968).

156. *Id.* at 21 (holding that the officer "must be able to point to specific and articulable facts" which warrant the intrusion).

there on a particular day. While using an Intelligent Transportation System to locate vehicles near the scene of a robbery might be "reasonably likely" to achieve an investigatory purpose, flying over large stretches of territory with a magnification camera to locate marijuana patches is not. Individualized suspicion is not required, but something more than a "Let's-see-what-we-can-find-here" attitude is.[157]

Nor should the mere assertion that surveillance will deter crime satisfy the definition. Presumably, overt surveillance by camera, plane, or other device would deter crime in any targeted area. However, unless the crime problem is significant, such surveillance is usually not legitimate under this definition.[158] To conclude otherwise would permit constant surveillance of virtually all nonprivate areas, with substantial detriment to privacy (in the sense of repose and anonymity), freedom of association, and most importantly, freedom from a sense of oppression. In short, the definitions of legitimate law enforcement objective (i.e., investigation, deterrence, prevention, protection from crime, and apprehension of criminals) and of how likely the achievement of that objective must be (i.e., when there are articulable reasons) are meant to provide meaningful, but at the same time relatively minimal, limitations on police conduct.

D. Standards Governing Specific Types of Surveillance

The final four standards provide specific guidelines for each of the five physical surveillance technologies.[159] As noted earlier, these standards represent application of the general principles, particularly Standard 2-6.1(c), setting out the competing law enforcement and privacy interests that must be balanced, and Standard 2-6.1(e), dealing with the appropriate decision-maker. Conversely, the general principles concerning implementation and accountability are replicated in the specific standards only when special considerations arise. In other words, when a specific standard states the conditions under which a given type of surveillance "is permissible," it is assumed that, in addition to the requirements listed in the standard, law enforcement officials will conduct surveillance in a nondiscriminatory manner, adhere to legitimate

---

157. As one court put it, "Law enforcement agencies should not have carte blanche power to conduct indiscriminate surveillance for unlimited periods of time of varying numbers of individuals." United States v. Curtis, 562 F.2d 1153, 1156 (9th Cir. 1977).

158. In some cases, authorities may wish to use overt (deterrence-driven) surveillance not because there have been a significant number of crimes in the targeted area, but because the few crimes that might occur will cause significant damage. The decision to set up cameras in Atlanta during the Olympics is a good example of this reasoning.

159. Illumination and telescopic devices are treated together. *See* Standard 2-6.5, *infra* Appendix.

objectives, appropriately document the surveillance, and so on. As with the discussion of the general principles, the specific standards will only be outlined here; discussion of the most controversial issues is left to Part III.

Standard 2-6.3, concerning video surveillance, contains three sections. Section (a) governs video surveillance of private locations, activities, and conditions. In accord with the holdings of most courts, this section places the same restrictions on video surveillance that are imposed on interception of private communications.[160] Since the ABA's standards governing communications surveillance are currently being revised,[161] the final content of section (a) is still unspecified, although it is clear that nonconsensual, non-exigent video surveillance of private areas will require a warrant based on probable cause.

Section (b) governs long-term overt video surveillance of nonprivate areas (e.g., cameras on telephone poles). This type of surveillance only need be reasonably likely to achieve legitimate law enforcement objectives. However, this determination must be made by either "a politically accountable law enforcement official or the relevant politically accountable governmental authority." Moreover, "the public to be affected by the surveillance" must be notified of "the intended location and general capability of the camera and [given] the opportunity, both prior to the initiation of the surveillance and periodically during it, to express its views of the surveillance and propose changes in its execution, through a hearing or some other appropriate means." Note that the standard limits public involvement to those "affected by the surveillance." This group would include those who live in or frequent the area to be surveilled but not the entire public, which might be insensitive to the intrusion represented by cameras in someone else's neighborhood.[162]

Section (c) governs all other video surveillance, meaning short-term overt video surveillance of nonprivate areas (e.g., videotaping a rally) and all covert video surveillance of nonprivate areas (e.g., installing hidden cameras to capture a pawn shop thief). Here too, meeting the

---

160. *See* LAFAVE, *supra* note 24. A few courts have held that only selected aspects of Title III apply to video surveillance. *See, e.g.*, United States v. Cuevas-Sanchez, 821 F.2d 248 (5th Cir. 1987); United States v. Biasucci, 786 F.2d 504 (2d Cir. 1986). For instance, the provisions of Title III that require applications to be signed by certain types of prosecutors and which limit electronic surveillance to certain crimes may not apply to video surveillance. For criticisms of these cases, see Kent Greenfield, Comment, *Cameras in Teddy Bears: Electronic Visual Surveillance and the Fourth Amendment*, 58 U. CHI. L. REV. 1045 (1991); Cheryl Spinner, Comment, *Let's Go to the Videotape: The Second Circuit Sanctions Covert Video Surveillance of Domestic Criminals*, 53 BROOK. L. REV. 469 (1987).

161. *See supra* note 12.

162. Note, however, that use of video surveillance in one area might merely displace activity to another, a possible argument for involving additional members of the public.

"reasonably likely to achieve a legitimate law enforcement objective" test is sufficient. However, the standard contemplates that in all non-exigent circumstances — in other words, most of the time — the decision as to whether this requirement is satisfied should be made by a supervisory official, not a field officer.

Standard 2-6.4, on tracking devices, also has three sections. Section (a) covers the installation of tracking devices. When such installation requires non-consensual entry into a private place, a law enforcement official must demonstrate probable cause to believe that the object to be tracked is in the place entered and that subsequent monitoring of the device will reveal evidence of a crime. The one exception to this rule is when the installation is "part of a systemwide program authorized by the legislature," a phrase meant to exempt installation of transponders in connection with Intelligent Transportation Systems; in this situation, legislative authorization is sufficient. An installation that does not require entry into a private place (e.g., placement of a beeper on the exterior of a car[163] or in an item belonging to the government)[164] need only meet the legitimate law enforcement objective test.

Section (b) governs the use of a tracking device to monitor movement. When the device is used "to determine whether or where the device is located within a particular private location," probable cause is required unless one of the subjects of the monitoring consents. In the latter case, and in all other cases of monitoring, the legitimate law enforcement objective test applies.

The practical effect of this standard is that police contemplating long-term, non-consensual tracking will often need probable cause because of the likelihood that, over an extended period, the tracked object will enter a home or similar private area. Of course, nothing in this standard prevents police with only an articulable law enforcement objective from using a device to track an item *to* a particular house.[165]

---

163. *Cf.* Cardwell v. Lewis, 417 U.S. 583, 591-92 (1974) (holding that taking paint scrapings from the exterior of a car does not infringe an expectation of privacy).

164. *Cf.* United States v. Jones, 31 F.3d 1304, 1310-11 (4th Cir. 1994) (holding that the monitoring of a beeper placed in government-owned property which a suspect then steals is not a search).

165. Both *United States v. Knotts*, 460 U.S. 276 (1983), and *United States v. Karo*, 468 U.S. 705 (1984), appear to hold that using a beeper to discover in what building an item is located (as opposed to its precise location) is not a search. In *Knotts*, 460 U.S. at 285, the beeper led police to a cabin but did not reveal movement of the beepered container within the premises. In *Karo*, 468 U.S. at 720-21, the beeper led police to a warehouse full of lockers, but did not reveal which locker contained the beeper. In neither situation did the Court find that the Fourth Amendment was implicated. Apparently, the rationale is that no personal right is violated until the police discover that the item is in a *specific* area associated with a reasonable expectation of privacy. *See* Clifford Fishman, *Electronic Tracking Devices and the Fourth Amendment: Knotts, Karo, and the Questions Still*

However, if the signal on a beeper is lost while the beeper is in a public place, probable cause is required to relocate the signal in a private place. Probable cause is also required if public tracking leads the police to an apartment building or a complex of buildings, so that identifying the precise apartment or building within which the item is located is impossible without resort to the tracking device.[166] For these reasons, under this standard seeking a warrant prior to tracking would often be the safest course even if installation in a private place is not required.[167]

Section (c) provides that when either installation or monitoring requires probable cause a judge must authorize that action in writing, except when there are exigent circumstances, in which case a judge should be consulted as soon as practicable. A court order may authorize monitoring for a maximum of sixty days "absent articulable facts demonstrating a need for longer surveillance." Extensions of sixty days may be authorized by a judge.

Standard 2-6.5 concerns illumination and telescopic devices. It is the most straightforward standard. For surveillance of private areas it requires probable cause and, in non-exigent circumstances, a warrant; it otherwise mandates adherence only to the legitimate law enforcement test. The one exception to the latter rule is when surveillance of nonprivate areas is "overt and not prolonged with respect to any given area," in which case no justification is necessary. Thus, the use of a Startron nightscope to look through a darkened bedroom window while hiding in bushes at the edge of a property would require probable cause and, unless exigency existed, a warrant, while the covert use of binoculars to observe a public square would only need to be reasonably likely to achieve a legitimate law enforcement objective, and the cursory use of a flashlight to illuminate bushes in a park or the exterior of a house would require no justification.

Standard 2-6.6 governs the use of detection devices. It consists of four sections. Section (a) concerns all detection devices, general and specific. In contrast to the rules governing other types of physical surveillance, a search of a private place using these devices is permitted on less than probable cause in a wide variety of situations, including whenever circumstances authorize a search incident to arrest, a search based on consent, an inventory search, a protective frisk, a search of an

---

Unanswered, 34 CATH. U. L. REV. 277, 341-46 (1985).

166. *Karo* stated that the use of a beeper to determine that a container is in a particular locker would be a search. *See* 468 U.S. at 720 n.6.

167. The government complained about this consequence in *Karo*, 468 U.S. at 718 ("[F]or all practical purposes [agents] will be forced to obtain warrants in every case in which they seek to use a beeper, because they have no way of knowing in advance whether the beeper will be transmitting its signals from inside private premises.").

entryway prior to an emergency entry, or a protective sweep of an arrestee's premises. In short, such devices may be used in any situation in which Fourth Amendment law allows a search on less than probable cause.[168] Further, the standard permits detection devices to be used at fixed checkpoints that serve "a compelling government interest" in preventing passage of contraband or weapons, as well as at temporary checkpoints when there is reasonable suspicion that the checkpoint will discover a person or instrumentality threatening "a substantial risk of death or bodily harm," or will discover a person or persons being threatened, as in a kidnaping victim.[169] Finally, when a detection device search does require probable cause, the standard eliminates the warrant requirement not only in exigent circumstances, but also when the place searched is associated with a "lesser expectation of privacy" (e.g., a car).[170]

Certain limitations are placed on detection-device checkpoints in Section (a)(iv). As with the rules governing long-term public video surveillance, a fixed checkpoint established to detect contraband or weapons must be approved by "an appropriate politically accountable law enforcement official or governmental authority"; further, the public affected by such a checkpoint must be notified of the location and be given periodic opportunities to express its views. A temporary checkpoint must be approved by a supervisory law enforcement official; additionally, the anticipated size of the group subjected to the checkpoint should be "reasonable in light of the purpose for which the device is to be used."

Section (b) of the detection device standard sets out additional situations in which detection devices that are *contraband-specific* may be used. Because these devices detect only contraband, their use is permitted whenever reasonably likely to achieve a legitimate law enforcement objective, even if the use entails search of a private place. The one exception to this rule is when the device is used to search a "place of residence," in which case probable cause (and a warrant in

168. *See* United States v. Robinson, 414 U.S. 218 (1973) (search incident to arrest); Schneckloth v. Bustamonte, 412 U.S. 218 (1973) (search upon consent); South Dakota v. Opperman, 428 U.S. 364 (1976) (inventory search); Terry v. Ohio, 392 U.S. 1 (1968) (protective frisks); Wilson v. Arkansas, 514 U.S. 927 (1995) (unannounced entry); Maryland v. Buie, 494 U.S. 325 (1990) (protective sweep incident to arrest).

169. *Cf.* Brinegar v. United States, 338 U.S. 160, 183 (1949) (Jackson, J., dissenting) (commenting how he would "candidly strive hard" to uphold a roadblock to save a kidnap victim even though the police had to "search every outgoing car," as "it might be reasonable to subject travelers to that indignity if it was the only way to save a threatened life").

170. *See* California v. Carney, 471 U.S. 386, 393 (1985) (noting a reduced expectation of privacy due to regulation of vehicles).

non-exigent circumstances) is required.[171] If the use of the device requires a seizure, grounds for the seizure must exist.[172]

Section (c) concerns weapon-specific devices. Unless these devices can be classified as contraband-specific (e.g., a gun-detection device in those jurisdictions where carrying a concealed weapon is illegal), this section subjects weapon-specific devices to the same restrictions as general detection devices. There is one exception: weapon-specific devices can be used in any circumstance in which protective action is permitted, "even absent any individualized suspicion of danger that otherwise would be required." Thus, if grounds for a stop are present, a weapon-specific device could be used to conduct an electronic "frisk" even if no suspicion of danger exists. When the search is narrowed to what a weapon-specific device detects, the fact that the officer does not actually harbor a suspicion of danger does not bar the search, despite the rule of *Terry v. Ohio*,[173] because the only intrusion into privacy is to identify whether there *is* potential danger.[174] For the same reason, this provision permits, without any articulable suspicion of danger, the use of a weapon-specific device to "look" beyond an entrance prior to an authorized entry, and to observe the vicinity of an arrest subsequent to the arrest.[175] Again, the theory is that in contexts where protective action would be authorized based on individualized suspicion, a device that detects only weapons can be used even absent that suspicion because it merely ensures that the protection occurs.

Finally, section (d) provides that law enforcement agencies should adopt procedures that address three implementation concerns. To the extent detection devices have the ability to "electronically strip" passersby,[176] procedures should be developed to allow the exposure of

---

171. *Cf.* United States v. Jacobsen, 466 U.S. 109, 140 (1984) (Brennan, J., dissenting) (inveighing against giving the police "free rein" to use such techniques to pry into the home).

172. As delineated in *Terry v. Ohio*, 392 U.S. 1 (1968), and its progeny.

173. 392 U.S. at 30 (permitting a frisk when the officer "reasonably [concludes] in light of his experience that criminal activity may be afoot and that the person with whom he is dealing may be armed and presently dangerous").

174. Further, the electronic frisk will usually be less intrusive than the traditional one. *See infra* note 284.

175. Because a post-arrest sweep of the immediate vicinity of the arrestee is already permitted in the absence of suspicion of danger, *see* Maryland v. Buie, 494 U.S. 325, 334 (1990), this provision adds nothing to law enforcement authority. *Buie* also permitted a protective sweep of other areas on the premises associated with a reasonable suspicion of danger. *See id.* Standard 2-6.6 would not permit *entry* into the surrounding area on less than reasonable suspicion, but it would allow beaming the device into the area from the point of arrest.

176. Although it does provide images of the body, the Millitech device described earlier, *supra* note 118 and accompanying text, purportedly does not reveal "intimate anatomical details." Dr. G. Richard Huguenin, Millitech Corporation, Testimony to the Crime and

anatomical information only to officers of the same gender. This section also cautions police against inappropriate use of "active" devices that may, through x-ray or other technology, cause physical harm to the target.[177] Finally and most importantly, it states that procedures should be adopted "to ensure that the capabilities of any device used conform as closely as possible to the authorized objective or objectives of the surveillance." If the objective in using a detection device is to find weapons, a weapon-specific device is preferable; if such a device is unavailable, police should use a general detection device that will achieve the objective with as little revelation of other information as possible.[178]

IV. AREAS OF CONTROVERSY

The foregoing description might have created the misleading impression that the discussion of the Task Force proceeded smoothly from one stage to another in crisp logical order. In fact, the group progressed in fits and starts, often backtracking. Preliminary versions of the specific standards were developed before the general principles were complete. Sections were added, deleted, and then added back in again; even the categories of physical surveillance subject to regulation changed.[179] Moreover, as might be expected within such a diverse group,[180] serious disagreements emerged. Indeed, virtually every provision of the standards was the subject of a debate over the two years of the project. Occasionally the Task Force came to an impasse, broken only at later meetings after further reflection.

The discussion below summarizes the most contentious debates, divided into twenty-one topics. It also provides, in more detail than previous parts of this Article, the rationale behind the provisions ultimately produced by the Task Force. In the end, all of these issues were resolved, if not to the complete satisfaction of each member of the

---

Criminal Justice Subcommittee of the House Judiciary Committee 3 (July 21, 1994) (on file with the *Harvard Journal of Law and Technology*). More powerful imaging techniques could reveal such details.

177. Devices that rely on radiation could be harmful under certain circumstances. *See id.* at 1.

178. This provision implements the least intrusive means principle of Standard 2-6.1(c)(iv).

179. *See supra* note 104.

180. *See generally* Alan Schwartz & Robert E. Scott, *The Political Economy of Private Legislatures*, 143 U. PA. L. REV. 595 (1995) (describing the dynamics of deliberations within American Law Institute rulemaking bodies).

Task Force, then at least sufficiently to permit each member to endorse the Tentative Draft.

Several issues debated by the Task Force could be termed "fundamental," in the sense that a failure to resolve them would have grounded the project. These issues, divided into four categories, are canvassed first; the rest of the Task Force's debates are discussed in the order in which they are raised by the standards.

A. Fundamental Issues

1. Mission Impossible: Technological Changes Will Render the Rules Moot

One objection to any project to develop rules governing technologically-assisted physical surveillance relies on the constant evolution of technology. Any effort at regulation, a few Task Force members initially argued, will soon be rendered obsolete by new developments in the field. Just as current detection devices were unimaginable thirty years ago, new devices that we cannot anticipate and therefore cannot intelligently regulate will be developed.

For a number of reasons, the Task Force quickly decided that this concern should not give it pause. First, inaction would only make matters worse. Legislative and administrative law in this area is almost non-existent, and courts' attempts to fill the void have been haphazard at best.[181] At the same time, the use of advanced technology to conduct physical surveillance is no longer an occasional occurrence; federal and state agencies use sophisticated illumination, telescopic, and detection devices with increasing frequency.[182] Devising some type of regulatory framework, even one that will require revision in the near future, is better than ignoring this burgeoning dimension of police investigation.[183]

Second, regardless of the technology involved, law enforcement needs (e.g., investigation and deterrence) and individual interests (e.g., privacy and freedom of association) do not change appreciably over time. New technologies might increase the tension between these needs

---

181. *See supra* Parts II.A & II.C.

182. *See supra* notes 2 & 3. *See also Brave New World*, TIME, Mar. 3, 1997, at 43 (describing new surveillance technology currently available).

183. *See* ARTHUR R. MILLER, THE ASSAULT ON PRIVACY 123 (1971) ("It would be unwise to deal with each new technological application on an individual basis divorced from the broader issues, or to delay until its privacy-invading excesses have come to pass."); Stephen L. Carter, *Technology, Democracy and the Manipulation of Consent*, 93 YALE L.J. 581, 584 n.14 (1984) (reviewing MARK G. YUDOF, WHEN GOVERNMENT SPEAKS: POLITICS, LAW AND GOVERNMENT EXPRESSION IN AMERICA (1983)) ("The fact that the danger has not made itself manifest does not mean that the danger does not exist.").

and interests, but would not diminish their fundamental relevance. Moreover, when new developments have necessitated new legal frameworks, the Fourth Amendment and related legal concepts have proven remarkably adaptable.[184]

Third, the decision to structure the standards around functional categories (e.g., tracking devices, telescopic devices, and detection devices) significantly mitigates the consequences of failing to anticipate a particular technology. These categories should encompass most new developments in physical surveillance.

2. Guidelines vs. Rules

A second core issue, which was not as easily resolved, concerned whether the Task Force's standards should be general guidelines or precise rules. This discussion, which persisted over several meetings, reflected the age-old debate whether law is best encapsulated in general or specific terms;[185] in particular, it flowed from two concerns about rules. The first concern was that detailed rules would not accommodate technological developments as easily as general guidelines. The second, and more vigorously pressed, concern was that precise rules are easy to violate inadvertently and thus more likely to lead to litigation and obstacles to legitimate law enforcement.

Opposing members of the Task Force believed that a project that produced only vague guidelines would not be worth the effort. Without relatively specific rules, they argued, the message of the standards would be muddled. At the least, this group felt the standards should strongly urge the police to produce specific rules.

In the end, the standards do not reflect the triumph of one of these positions over the other, but rather a compromise between the two. The general principles of Standard 2-6.1 are more like guidelines, while the remaining standards more closely resemble rules. However, even the latter standards are broad in scope. Most obviously, the multi-factor definition of privacy and the relatively open legitimate law enforcement objective test leave considerable room for discretion. In a number of other standards, the Task Force again opted for language that avoids

184. For instance, the advent of wiretapping and bugging initially created difficult analytical problems for the Supreme Court, since conversations are not "persons, houses, papers or effects" and cannot be "seized" in the same way these items can. *See* Katz v. United States, 389 U.S. 347, 365-66 (1967) (Black, J., dissenting). Nonetheless, the *Katz* majority's adoption of a privacy analysis allowed constitutional regulation of an investigative technique not anticipated by the Framers. *See id.* at 353.

185. *Cf.* Duncan Kennedy, *Form and Substance in Private Law Adjudication*, 89 HARV. L. REV. 1685 (1976) (exploring the advantages and disadvantages of clear but rigid rules and amorphous but adaptable standards).

straitjacketing law enforcement.[186] But at the same time, Standard 2-6.1(g) admonishes law enforcement agencies to devise more specific rules implementing these standards.

3. Fourth Amendment Redux or Comprehensive Effort?

A third basic issue was raised by the suggestion from some members of the Task Force that the group merely try to summarize Fourth Amendment law, without reaching subconstitutional issues. As with the argument in favor of guidelines, this stance was motivated by a desire to avoid undermining legitimate law enforcement efforts.

The response to the latter argument was less equivocal, however. As the preceding description of the standards makes clear, the Task Force made an effort to tackle all the issues raised by law enforcement use of physical surveillance, not just those addressed by courts. The Task Force concluded that it could not justify the implication of a simple summary of Fourth Amendment law: that the vast amount of surveillance not meeting the "search" threshold[187] should not be regulated at all. For instance, given its Orwellian overtones, most people would probably agree that placement of video cameras on street corners requires some type of limitation, despite its apparent immunity from constitutional strictures.[188] Similarly, as Part II.C explained, a number of issues regarding implementation and accountability are not addressed by constitutional doctrine, but are important to any comprehensive regulatory system.

Furthermore, the seemingly simple goal of describing current Fourth Amendment law on physical surveillance may not be achievable, for even when courts *have* regulated technologically-assisted physical surveillance, their holdings have not been models of clarity. The Supreme Court alone has proffered several different analytical approaches.[189] When one looks at lower courts, the variety in holdings and rationales assumes bewildering proportions. For example, some courts

---

186. *See infra* text accompanying notes 209-16 (notice), 217-25 (disclosure and retention of records), 226-31 (documentation of surveillance decisions), & 232-33 (public dissemination of types of surveillance conducted).

187. *See supra* Part II.A.

188. *See, e.g.*, Michael Cooper, *With Success of Cameras, Concerns Over Privacy*, N.Y. TIMES, Feb. 5, 1997, at B4 (describing the questionable efficacy of cameras in some areas and the concerns of some civil libertarians about an Orwellian society); Timothy Egan, *Police Surveillance of Streets Turns to Video Cameras and Listening Devices*, N.Y. TIMES, Feb. 7, 1996, at A12 (discussing, *inter alia*, concerns about video viewing of homes, maintenance of recordings, and audio capability).

189. *See supra* Part II.A.

have concluded that thermal imaging of a building requires a warrant,[190] while others have declared that this activity does not even implicate the Fourth Amendment.[191] Similarly, some courts have held that the use of binoculars to look inside a building is a search,[192] while others have said it is not.[193]

In short, legislators, policymakers, police, attorneys, and trial judges need more guidance than presently provided on both constitutional and subconstitutional issues. The standards endeavor to provide that guidance, both with specific rules and with a statement of the competing values at stake.

4. The Relationship of Public and Private Surveillance

A fourth fundamental issue was whether the restrictions placed on the police should be greater than those placed on the public. According to one view, if a private citizen can use a video camera to record activity on a public street with no restrictions, the police should be able to do so as well. Because private surveillance of public places is virtually unregulated, the practical consequence of this position is almost identical to the stance that standards should reflect only Fourth Amendment law.

One response to this position is, rather than foregoing restrictions on the police, to limit all technologically-assisted physical surveillance, public and private. After all, use of these devices by fellow citizens can have a significant impact on privacy and freedom of action. Furthermore, private use of physical surveillance technology has increased enormously in recent years. Indeed, corporate and personal use of video cameras, telescopic devices, and other types of physical surveillance technology is probably outpacing use by the government. Perhaps the model provided by communications surveillance law, which bars the private use of communications interception equipment,[194] should be followed here as well.

---

190. *See, e.g.*, United States v. Field, 855 F. Supp. 1518 (W.D. Wis. 1994); *see also infra* note 281.

191. *See, e.g.*, United States v. Kyllo, 1996 WL 125594 (D. Or. 1996); United States v. Penny-Feeny, 773 F. Supp. 220, 226-28 (D. Haw. 1991), *aff'd on other grounds*, 984 F.2d 1053 (9th Cir. 1993).

192. *See, e.g.*, People v. Oynes, 920 P.2d 880 (Colo. Ct. App. 1996); State v. Carter, 790 P.2d 1152 (Or. Ct. App. 1990).

193. *See, e.g.*, People v. Arno, 153 Cal. Rptr. 624, 629 (Ct. App. 1979).

194. *See* 18 U.S.C. § 2512 (1994) (outlawing manufacture, distribution, possession, and advertising of certain wire, oral, or electronic communications surveillance devices).

Nonetheless, with one possible exception,[195] the standards do not attempt to control the private use of physical surveillance devices.[196] Given the legitimate purposes that such devices may serve, and their prolific usage by the general population, any attempt to achieve such control in a sensible manner would be a significant undertaking best left to other groups.[197]

Thus the question for the Task Force remained whether the standards should impose limitations on activity by the police that ordinary citizens can perform with impunity. For instance, though use of Startron binoculars to peer into a private area might trigger a tort or privacy law action,[198] surveillance of public areas is not likely to bring any legal sanction. Accordingly, some members of the Task Force wondered why police should have to abide by even minimal restrictions on their surveillance of public places.

The Task Force concluded, however, that the government's vast resources and its power to deprive people of freedom distinguish it from private actors. The Bill of Rights limits state action, not private action.[199] Put another way, a democratic government must trust its citizens in order to earn its citizens' respect.[200] The government shows no trust if it indiscriminately uses its power against the citizenry. Regardless of what

---

195. At present, the Electronic Surveillance Standards recommend the imposition of criminal penalties for the "possession, sale, distribution, advertisement or manufacture of a device the design or disguise of which makes it primarily useful for the surreptitious overhearing or recording of... communications." Electronic Surveillance Standards, *supra* note 7, Standard 2.1(b)(iv). Given the linkage imposed by Standard 2-6.3(a) between video surveillance of private locations and the Electronic Surveillance Standards, a person who possesses a video device designed primarily for covert observation of private activities (e.g., a teddy bear camera) or who uses such a device covertly might be committing a crime. In light of this possible result, whether the Task Force will retain this linkage remains to be seen.

196. The proposed standards avoid explicitly addressing government use of information collected through private physical surveillance. *Cf.* United States v. Jacobsen, 466 U.S. 109 (1984) (discussing when replication of a private search by a public actor is a Fourth Amendment search); Walter v. United States, 447 U.S. 649 (1980) (same).

197. The ABA Criminal Justice Section Council has just established a Task Force on Policing Privatization, which might consider such issues. Letter from Michael Johnson, Chair, Criminal Justice Standards Committee, to Members, Policing Privatization Task Force (Apr. 9, 1997) (on file with the *Harvard Journal of Law and Technology*).

198. "Several successful actions for invasion of privacy have been brought against defendants who have utilized secret video cameras, see-through panels, peepholes, hidden microphones, or window-peeping." H. Morley Swingle & Kevin M. Zoellner, *Criminalizing Invasion of Privacy: Taking a Big Stick to Peeping Toms*, 52 J. Mo. B. 345, 346 (1993).

199. *See, e.g.*, Burdeau v. McDowell, 256 U.S. 465 (1921).

200. *Cf.* Sundby, *supra* note 124, at 1755 (1994) (arguing that the fundamental purpose of the Fourth Amendment and of "maintaining a constitutional system" is the promotion of "government-citizen trust").

private individuals may be able to do, self-interest mandates that the government refrain from arbitrary, unjustifiable surveillance.[201]

B. General Principles

5. Is Privacy Invasion All We're Worried About?

The Task Force expended considerable energy on the phrasing of sections (a) and (b) in Standard 2-6.1 — which state the reasons why physical surveillance technology is needed and why it may need to be regulated — because these sections set the stage for the rest of the standards. This effort was aimed at making these important sections as comprehensive and clear as possible. There was little disagreement about content.

However, one substantive issue did arise in connection with section (b). The penultimate draft of this section included a more detailed recitation of values that might be diminished by unregulated physical surveillance. In addition to talking about the "chilling effect" that technologically-assisted physical surveillance might have upon "constitutionally protected activities, such as freedom of speech, association, or travel," the earlier draft stated that regulation is needed when such surveillance would pose "a significant infringement of other widely shared values in a democratic society, including the enjoyment of anonymity and places of repose, the absence of a pervasive police presence, and the absence of intensive official scrutiny except in response to suspicious conduct."[202] Some members of the Task Force successfully objected to the inclusion of this language on the ground that it was too vague and might lead to the regulation of innocuous law enforcement behavior. Because the deleted language captures interests that are not clearly encompassed by the privacy concept, this objection came close to reprising the idea that the standards should deal only with Fourth (and First) Amendment concerns.

---

201. This reasoning might suggest that the standards should govern *all* government use of technologically-assisted physical surveillance. However, such surveillance comes in many guises that are not subject to easy categorization: secret service agents charged with protecting federal officials; national security organizations designed to ferret out terrorists; regulatory bodies obligated to monitor public health and safety; and transportation and court agencies concerned with protecting those who use their facilities. Rather than address the complex issues that arise in these varied contexts, the introduction to the standards will make clear that the term "law enforcement" as used in the standards is meant to encompass only the last-named area plus typical police and detective work.

202. Standard 2-6.1(b) (draft of Feb. 10, 1997) (on file with the *Harvard Journal of Law and Technology*).

The practical effect of the deletion is probably trivial, however. Very little technologically-assisted physical surveillance is left unregulated by the specific standards.[203] While much surveillance may take place upon the minimal showing required by the legitimate law enforcement objective test, this test, along with the implementation and accountability provisions, imposes some limitations on even routine use of surveillance devices in nonprivate areas. Furthermore, the current phrasing of section (b) refers not only to privacy and First Amendment freedoms, but also to the "openness of society" as a value worthy of protection.

6. Should the Use of the Least Intrusive Device be Required?

When deciding whether a particular type of surveillance should take place, some members of the Task Force thought that the use of the least intrusive technique should be mandated, or at least strongly encouraged. As technological advances make more intrusive surveillance alternatives available, these members argued that the need to avoid "investigative overkill" becomes greater.[204] Further, while previously the most intrusive alternatives were also the most time-consuming and expensive ones — so that the least intrusive alternative was typically selected as a matter of efficiency — technology now provides options that are highly intrusive but relatively inexpensive and not manpower intensive. For instance, putting a cop on every corner is fiscally impossible for most jurisdictions; putting a camera on each block may not be.

At the other end of the spectrum, some members of the Task Force expressed significant antipathy toward any reference to the least intrusive means concept, noting that the Supreme Court has explicitly refused to endorse this requirement in the Fourth Amendment context.[205] They also voiced concern that such a limitation would require police to make difficult decisions about relative intrusiveness which might relegate investigative effectiveness to a secondary role. For instance, how does one evaluate whether a video camera on a telephone pole is less intrusive than a police officer on every street corner, and of what relevance is the fact that the latter method of surveillance is much more expensive?

---

203. The only obvious example is overt, unprolonged use of telescopic and illumination devices. *See* Standard 2-6.5(b)(I), *infra* Appendix.

204. *See supra* Part I.

205. *See, e.g.*, Illinois v. Lafayette, 462 U.S. 640, 647 (1983) ("The reasonableness of any particular governmental activity does not necessarily or invariably turn on the existence of alternative 'less intrusive' means."); United States v. Martinez-Fuerte, 428 U.S. 543, 556 n.12 (1976) ("The logic of such elaborate less-restrictive-alternative arguments could raise insuperable barriers to the exercise of virtually all search-and-seizure powers.").

The Task Force decided that Supreme Court case law, as well as pragmatic law enforcement and economic considerations, require a measured approach. Thus, the standards indicate that relative intrusiveness should be a consideration but not a dispositive criterion, in selecting a particular technology.[206] Further, relative intrusiveness is to be evaluated in light of other "available effective and efficient alternatives"[207]; law enforcement is not required to sacrifice effectiveness or to ignore resource constraints in deciding whether a particular surveillance technique is permitted.[208]

7. Should People Know They've Been Watched?

Under both the Electronic Surveillance Standards[209] and federal law,[210] post-surveillance notice of wiretapping and bugging must be given to all those listed on the warrant application. Initially the Task Force's standards mandated the same requirement for all covert physical surveillance that requires probable cause (e.g., surveillance of the interior of a home).[211] As in the communications surveillance context, [212]the

---

206. *See* Standard 2-6.1(c)(iv), *infra* Appendix.

207. *Id.*

208. For a critique of this approach, see Nadine Strossen, *The Fourth Amendment in the Balance: Accurately Setting the Scales Through the Least Intrusive Alternative Analysis*, 63 N.Y.U. L. REV. 1173 (1988).

209. Standard 5.14 of the Electronic Surveillance Standards, *supra* note 7, provides:

> As soon as practicable but not later than ninety days after the return is made to the judicial officer . . . the judicial officer should cause to be served on the person named in the order of authorization or approval or the application for such an approval . . . an inventory which should include notice of—
>
> (i) the entry of the order or the making of the application;
>
> (ii) the date of the entry of the order or of the denial of the application;
>
> (iii) the period of authorized, approved or disapproved overhearing or recording;
>
> (iv) the overhearing or recording, if any, of communications; and
>
> (v) the period, if any, of actual overhearing or recording.
>
> Upon a showing of good cause made to the judicial officer, the serving of the inventory should be postponed.

210. *See* 18 U.S.C. § 2518(8)(d) (1994).

211. *See* Standard 2-6.1(d)(iv)(B) (draft of Nov. 16, 1996) (on file with the *Harvard Journal of Law and Technology*).

212. The commentary to the PROJECT states:

> The possibility of surreptitious surveillance is, of course, the most telling objection to any system of permissive use. An inventory procedure removes most of the source of that objection. When an individual receives the inventory he will, moreover, then be in a position to take whatever action is available to him to suppress, if

primary reason for this rule was that the intrusion associated with such surveillance is significant, yet usually undiscovered by the target unless prosecution takes place. Even when a warrant is sought and a judge reviews the surveillance decision, a notice requirement provides effective disincentives to questionable conduct because the police know their targets are more likely to learn of misconduct. When the surveillance does not require a warrant, a notice requirement is even more important because no one will discover any abuse of discretion unless prosecution takes place, in which case the effect of hindsight bias will often favor the police.[213] As noted earlier,[214] notice in probable cause situations might even be constitutionally required under *Berger v. New York*.[215]

However, some members of the Task Force and several police organizations were worried that post-surveillance notice would burden law enforcement, or prematurely alert a suspect and foil an investigation (especially in conspiracy and similar investigations). The latter concern could presumably be addressed through language, like that found in electronic surveillance laws, that allows post-surveillance notice to be postponed for good cause.[216] Nonetheless, the Task Force decided that the standards should merely require "reasonable notice" of covert surveillance and that the commentary to the standards should flesh out the competing interests involved.

8. Disclosure and Retention of Surveillance Results

The recording ability of physical surveillance technology, particularly in connection with video surveillance and Intelligent Transportation Systems, raises the potentially difficult issues of disclosure and retention. Consider two examples in addition to those given earlier.[217] First, suppose the government conducts surveillance of a business to determine whether drug importation laws are being violated. Assuming the surveillance is legally justified, the use of any information obtained is certainly permissible in a criminal prosecution on drug importation or

---

possible, the evidence obtained or to recover, where appropriate, civil damages.

PROJECT, *supra* note 7, at 161-62 (citation omitted).

213. *Cf.* JEROME SKOLNICK, JUSTICE WITHOUT TRIAL: LAW ENFORCEMENT IN DEMOCRATIC SOCIETY 221, 223-24 (2d ed. 1975) (noting that when searches uncover incriminating evidence, courts' perceptions of the reasonableness of such searches shift in favor of the police).

214. *See supra* text accompanying note 133.

215. 388 U.S. 41 (1967).

216. Standard 5.14 of the Electronic Surveillance Standards permits postponement upon "a showing of good cause," see *supra* note 208, requiring law enforcement to show how the inventory will damage an investigation.

217. *See supra* text accompanying note 92.

related charges. However, the information might also be sought by other government agencies (e.g., an environmental protection unit), by competitors, or by private news organizations. As another example, suppose a school's video surveillance tapes of its halls are sought by police investigating criminal activity.[218] Should disclosure be automatic in these situations? If not, what rules should govern the disclosure and retention of surveillance records?

Because these questions involve obtaining pre-existing information, they are best answered by standards governing transactional surveillance.[219] However, the Task Force believed that the physical surveillance standards should at least touch upon the disclosure and retention issues for two reasons. First, the propriety of a search or seizure depends in part upon what is done with the information obtained. Even if the police have probable cause to search a house, a decision to display all of its contents in the public square is unreasonable. Second, dissemination of information is itself an invasion of privacy. Such dissemination may be permissible if consistent with the purpose of a duly authorized search, but a violation of privacy rights may occur if the information obtained is used for other purposes.

Starting from this premise, an earlier version of the standards provided that disclosure of surveillance results "should be permitted only for purposes consistent with the purpose of the surveillance or those collateral uses determined to be lawful by previously promulgated statute, court decision or regulation."[220] The rationale for this approach is threefold: (1) legislative, judicial, or agency action is more likely to be based on consideration of all the complex state and individual interests involved;[221] (2) disclosures motivated by discriminatory or vindictive motives are less likely; and (3) judicial review of any disclosure decision is facilitated.[222]

An earlier version of the standards also proposed that records should be destroyed after being used for their intended purpose or when that

---

218. This issue was expressly avoided by the Supreme Court in *New Jersey v. T.L.O.*, 469 U.S. 325, 333 n.3 (1985).

219. For a definition of this term, see *supra* note 13 and accompanying text.

220. *See* Standard 2-6.1(d)(vi) (draft of Feb. 10, 1997) (on file with the *Harvard Journal of Law and Technology*).

221. As the Court recognized in *Michigan Dep't of State Police v. Sitz*, 496 U.S. 444, 453-54 (1990), the reasonableness of a search is significantly enhanced if the governing rules come from legislative or high administrative officials rather than the street police themselves, and if the police are given relatively little discretion in construing these rules.

222. *See* Harold J. Krent, *Of Diaries and Data Banks: Use Restrictions Under the Fourth Amendment*, 74 TEX. L. REV. 49, 85-92 (1995).

purpose is "no longer likely to be achieved."[223] This provision was based on a similar rationale. If a duly promulgated law requires retention of the records, presumably some public debate about the propriety of such action has taken place. However, if no such law exists then the proposal would have required their destruction in the indicated circumstances. Fearful of extensive video libraries that would retain information on vast numbers of individuals in perpetuity, some members of the Task Force argued that even this protection was not enough and that records should be destroyed after a fixed time, regardless of their potential use.

All of these proposals were rejected by the Task Force because they might prohibit or render impossible the use of highly probative information simply because the use was not anticipated by law. Accordingly, the language submitted to the Criminal Justice Section Standards Committee[224] merely required that disclosure be "for lawful purposes," which suggests that disclosure and retention are permitted so long as not *prohibited* by a statute or regulation. The Committee added the word "designated" before the word "lawful" to indicate that, contrary to the Task Force's formulation, some legal authorization should exist, at least for disclosure.[225] However, given the ambiguity of the word "designated," such legal authorization might consist simply of a directive by a supervisor to disclose particular information.

A final related issue should be noted. Assuming that adequate protection against inappropriate disclosure to non-law enforcement entities exists, a few members of the Task Force argued that if these disclosure rules are strictly adhered to, other restrictions on covert surveillance could be minimized. This position assumes that the surveillance itself, because undetected by the targets, does not harm any individual interests, and that disclosure of results, because limited to law enforcement purposes and other authorized objectives, does not harm innocent people.

The second assumption, at least, is erroneous. Even if the surveillance results are used only against the guilty, the knowledge that the government is conducting covert surveillance without restraint would ultimately affect everyone's sense of security. Further, if information is

---

223. *See* Standard 2-6.1(d)(vii) (draft of Feb. 10, 1997) (on file with the *Harvard Journal of Law and Technology*) ("Protocols should be developed for the destruction of surveillance records not required to be maintained by law. Such records should be destroyed (A) after they are used for their intended purpose, or (B) when that purpose is no longer likely to be achieved.").

224. Recall that the Committee is the first layer of review in the ABA's standards review process. *See supra* note 14. In its February, 1997 meeting, the Committee began its discussion of the standards. The change reported in the text below was one outcome of this meeting.

225. *See* Standard 2-6.1(d)(vi), *infra* Appendix.

disclosed for purposes other than law enforcement, even if pursuant to a pre-existing rule, the privacy of innocent people may be infringed. Thus, while proper precautions regarding disclosure can minimize the injury to privacy, they do not obviate the need for standards requiring justification for a particular surveillance.

9. Is Documentation Necessary to Articulation?

When surveillance is based on probable cause, the reasons for the surveillance will normally be documented in a warrant application and thus be available for judicial or administrative review.[226] However, for searches conducted without a warrant due to exigent circumstances, no such application will exist and a separate written record of the decision to search may not be created. Law enforcement officers are even less likely to record their reasons for acting when subconstitutional conduct not requiring probable cause is involved.

To ensure that the reasons for surveillance are "articulated" when a warrant is not required and to assist in periodic review of surveillance usage, some members of the Task Force proposed a documentation requirement. Thus, an earlier version of the standards provided for documentation identifying the official or officials responsible for the decision to conduct particular surveillance.[227] Moreover, this earlier version required that the reasons for the surveillance be documented, except when the surveillance decision was made by a field officer and the surveillance was "cursory."[228]

This earlier version was rejected in favor of the current formulation, which requires administrative rules to ensure that "the information

---

226. *See, e.g.*, FED. R. CRIM. P. 41.

227. *See* Standard 2-6.1(f)(I) (draft of Feb. 10, 1997) (on file with the *Harvard Journal of Law and Technology*).

228. *See* Standard 2-6.1(f)(ii) (draft of Feb. 10, 1997) (on file with the *Harvard Journal of Law and Technology*). The relevant text read:

> (f) *Accountability and Control.* Government officials should be held accountable for use of regulated technologically-assisted physical surveillance technology by means of:
>
> (i) Documentation of the official or officials responsible for the decision to conduct particular surveillance.
>
> (ii) Documentation of the reasons for the surveillance. Where the final decision to conduct particular surveillance is made by a nonsupervisory law enforcement officer, and the surveillance is not cursory in nature
>
> (A) that officer should make a contemporaneous record articulating the basis for undertaking the surveillance and noting the duration of the surveillance, and
>
> (B) such records should periodically be reviewed and evaluated by a supervisory law enforcement officer.

necessary for [official] accountability be maintained."[229] Again, the concern that onerous, litigation-producing, and perhaps useless burdens might be placed on law enforcement officers won the day over the more stringent rule. For instance, some members of the Task Force thought requiring field officers to record every prolonged use of binoculars would not appreciably protect privacy but could lead to obfuscating defense objections when such records were incomplete or non-existent. The current language is thus not as specific as the earlier version regarding the precise information that must be maintained. However, it does require departments to keep some accountability information, perhaps at least a record of how a particular surveillance was conducted and of who conducted it.

On the issue of accountability, early on the Task Force unanimously agreed that exclusion of evidence is an appropriate remedy only when the Fourth Amendment is violated. In all other situations, disincentives should depend upon administrative and other sanctions. Thus, the standards do not impose a statutory exclusion remedy of the type found in the original version of the Electronic Surveillance Standards[230] or Title III.[231]

10. Giving Away Police Secrets

Considerable debate focused on whether law enforcement should periodically disseminate to the public statistics about the frequency of technologically-assisted physical surveillance, as it must under the law governing wiretapping and bugging.[232] On the one hand, the public and its representatives cannot intelligently assess the scope and impact of technologically-assisted physical surveillance without information of this sort. On the other hand, law enforcement agencies do not want to alert potential criminals to specific techniques; indeed, there is perhaps an inclination on the part of law enforcement to keep the public ignorant of

---

229. *See* Standard 2-6.1(f)(I), *infra* Appendix.

230. *See* Electronic Surveillance Standards, *supra* note 7, Standard 2.3(c) (permitting a suppression motion by "any party aggrieved by the overhearing, recording, use, or disclosure of such communications or evidence derived therefrom"). An earlier version of this standard that required exclusion only when "substantial rights" are violated was removed by the 1986 amendments.

231. Title III requires exclusion in a number of situations in which the Fourth Amendment probably would not. *See, e.g.*, 18 U.S.C. § 2517(5) (1994) (allowing exclusion for failure to disclose to the judge the interception of communications not related to the offense specified in the wiretap order "as soon as practicable"); 18 U.S.C. § 2518(8) (1994) (allowing exclusion for failure to seal recordings); 18 U.S.C. § 2518(9) (1994) (allowing exclusion for failure to provide an inventory at least 10 days before trial).

232. *See supra* note 101.

the use of covert surveillance technology.[233] As a compromise, the current standard requires public dissemination of the frequency of use in terms of the general surveillance categories created by these standards (e.g., private video surveillance, public video surveillance, and tracking devices). Particular technologies need not be revealed.

C. Definitions

11. The Legitimate Law Enforcement Objective Standard

Part II demonstrated that the Fourth Amendment imposes no limitations on many types of surveillance of public places.[234] Nonetheless, earlier versions of the standards endorsed a reasonable suspicion requirement in a number of public surveillance contexts.[235] Behind these restrictions was the belief that surveillance of public activity could have particularly intrusive or oppressive consequences in these situations.[236] However, as noted earlier,[237] many members of the Task Force thought that, given the courts' lack of action in this area, such surveillance should be essentially unregulated. The compromise which emerged was the "reasonably likely to achieve a legitimate law enforcement objective" test, which is meant to impose minimal, but meaningful, justificatory conditions on surveillance of nonprivate areas.[238]

---

233. *See* Richard McAdams, *Tying Privacy in Knotts: Beeper Monitoring and Collective Fourth Amendment Rights*, 71 VA. L. REV. 297, 328 n.145 (1985) (noting the difficulty of determining how often beeper surveillance occurs given the lack of records and the reluctance of police to keep or disclose such records).

234. *See supra* Part II.A.

235. *See* Standard 2-6.3(c) (draft of Aug. 5, 1996) (on file with the *Harvard Journal of Law and Technology*) (requiring, with respect to covert video surveillance, either reasonable suspicion or documentation of the "expected frequency" of the "particular type of criminal activity" and "that other methods of deterrence would be less effective"); Standard 2-6.4(b)(ii) (draft of Oct. 28, 1996) (on file with the *Harvard Journal of Law and Technology*) (requiring reasonable suspicion for the monitoring of a beeper in nonprivate areas); Standard 2-6.5(b) (draft of Aug. 5, 1996) (on file with the *Harvard Journal of Law and Technology*) (requiring reasonable suspicion for the use of illumination and telescopic devices to view nonprivate areas).

236. For instance, because targets are unaware of its occurrence and thus cannot take steps to minimize exposure, covert surveillance may well reveal far more intimate detail than overt video surveillance. For discussion of the rationale for imposing a reasonable suspicion requirement in connection with the tracking of public movements, see *infra* note 268.

237. *See supra* text accompanying notes 187-93.

238. For an argument that reasonable suspicion should be required for surveillance "intrusions" amounting to less than a Fourth Amendment search, see Lewis R. Katz, *In Search of a Fourth Amendment for the Twenty-first Century*, 65 IND. L.J. 549 (1990).

Although this phrase requires that the law enforcement objective be "articulable," some members of the Task Force believed that the standard was still too amorphous. In an effort to make the test somewhat more restrictive and concrete, one version of the definition explicitly required that the police be able to articulate a particular crime or type of crime they hoped to deter, prevent, or investigate, or a "substantial" crime problem that required deterrence.[239] The Task Force was concerned, however, that such an addition might prevent clearly reasonable surveillance (e.g., use of video cameras to scan the Olympic Park in Atlanta). At the same time, it directed that the commentary to the definition endorse particularity and substantiality as two of the criteria for determining reasonableness.[240]

12. The Definition of Privacy

Much discussion centered around how the Task Force should define those situations that warrant the first tier of protection (i.e., those that require probable cause). For instance, an early version of the standards referred to the first-tier domain as a "home or similar location."[241] Another approach discussed, but never put into draft language, required justification based on the sophistication of the device in question. However, the Task Force, like the courts, came to see privacy as a multi-factor concept, and thus ultimately defined privacy by simply listing relevant considerations. Although this approach obviously lacks the clarity that the Task Force had hoped to provide, the group concluded that it was the best way to define privacy: there are simply too many permutations involving technology to permit bright-line statements about

---

239. *See* Standard 2-6.2(e) (draft of Oct. 28, 1996) (on file with the *Harvard Journal of Law and Technology*). The relevant text read:

> (e) *Legitimate law enforcement objective.* Investigation, deterrence or prevention of an offense defined by statute, and prevention of other physical harm. An action by a law enforcement officer is "reasonably likely to achieve a legitimate law enforcement objective" if there are articulable reasons for concluding that the action will:
>
> (i) discover the commission of a particular offense or type of offense;
>
> (ii) further an ongoing investigation of a particular offense or type of offense;
>
> (iii) deter or prevent a particular offense;
>
> (iv) deter a significant number of offenses in a given area; or
>
> (v) prevent one or more persons from suffering serious physical harm.

240. *See supra* text accompanying notes 153-58.

241. *See* Standards 2-6.3 to 2-6.7 (draft of Oct. 28, 1996) (on file with the *Harvard Journal of Law and Technology*).

activities or conditions that deserve the Constitution's greatest protection.

Consider one illustration of the problem. As indicated above, one possible definition would have been to declare the interior of the home and similar locations "private," thereby dictating that such locations can never be observed without probable cause. While this approach would be easy to apply and would even come close to describing Fourth Amendment law, it would foreclose — unless probable cause existed — enhanced surveillance from a public sidewalk of activity taking place directly in front of uncurtained windows and open front doors, even if only a flashlight or video camera was used in the observation. Although there are good reasons to be reluctant to give much weight to such circumstances,[242] both case law and logic demand that they be given some effect. Thus, the definition adopted incorporates the courts' admittedly vacillating positions on what is private and what is not.[243]

D. Video Surveillance

13. Unresolved Issues Involving Surveillance of Private Locations

Because the ABA's revised standards on communications surveillance have yet to be finalized, section (a) of the video surveillance standard, which equates video surveillance of private locations with interception of private communications, leaves a number of questions unanswered. Four issues are canvassed here, but are not resolved.

First, should there be a provision regulating the installation of surveillance devices? Both the Electronic Surveillance Standards and Title III avoid the issue. Further, in *Dalia v. United States*,[244] the Supreme Court explicitly held that a separate warrant is not required for an entry to install eavesdropping equipment, although the entry must be "reasonable."[245] Yet a good argument can be made that the Fourth Amendment requires a probable cause finding that non-consensual entry

---

242. *See supra* Part II.B.

243. Another regulatory approach would be to prohibit certain types of surveillance in certain situations (e.g., no satellite surveillance of homes, no use of detection devices to see through clothing). Given society's willingness to permit electronic eavesdropping, which may be even more intrusive than the examples just given, this categorical approach seems overly restrictive. That being said, it should be noted that the flexible approach adopted here is not necessarily inconsistent with barring the most intrusive types of surveillance or making them extremely difficult to justify. In other words, application of the factors in Standard 2-6.1(c) might lead to a conclusion that certain types of surveillance are not justified by any legitimate law enforcement objective.

244. 441 U.S. 238 (1979).

245. *See id.* at 258 (holding that "the manner in which a [surveillance] warrant is executed is subject to later judicial review as to its reasonableness").

into a home is necessary to gather criminal evidence, whether in the communications or physical surveillance context.

Second, the Electronic Surveillance Standards[246] and Title III[247] state that a wiretap order may not be issued unless a judge finds that normal investigative procedures have been tried and failed, or are likely to be unsuccessful or too dangerous. This "necessity" requirement was designed to keep electronic surveillance a last resort, given its intrusiveness.[248] With the advent of video surveillance, however, it is not clear how the necessity requirement works. As currently written, the Electronic Surveillance Standards require the police to use video surveillance (presumably with no audio capability) before resorting to a wiretap or a bug. Yet visual surveillance can be as intrusive or more intrusive than aural surveillance.[249]

A third issue of this sort concerns minimization. The current ABA standards on aural surveillance state that the judicial order authorizing surveillance shall contain "a directive that overhearing or recording shall be conducted in such a way as to minimize the overhearing or recording of conversations not otherwise subject to overhearing or recording."[250] Federal law is similar in vein,[251] although the Supreme Court's interpretation of this provision significantly emasculates even this relatively vague

---

246. *See* Electronic Surveillance Standards, *supra* note 7, Standard 2-5.4(c) (requiring a finding that "other investigative procedures have or had been tried and have or had failed or reasonably appear or appeared to be unlikely to succeed if tried or to have been or to be too dangerous").

247. *See* 18 U.S.C. § 2518(3)(b) (1994) (requiring a finding that "normal investigative procedures have been tried and failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous").

248. As the commentary to the PROJECT indicates, the Supreme Court itself states in *Berger v. New York*, 388 U.S. 41, 60 (1967), that a special showing is "more important in eavesdropping, with its inherent dangers, than that required when conventional procedures of search and seizure are utilized." PROJECT, *supra* note 7, at 140.

249. But this is not necessarily the case, depending upon what is viewed or heard. This is why the proposals that place greater limitations on video surveillance are also suspect. *But see* Greenfield, *supra* note 158, 1057-77 (suggesting, *inter alia*, (1) that video surveillance should be authorized for fewer types of crimes than is the case with aural surveillance, (2) that video surveillance should be permitted only if aural surveillance first indicates criminal activity is occurring, (3) that video surveillance should be permitted only if the judge identifies the person to be observed (which is required for aural surveillance only if the person is known), (4) that the court order for video surveillance should be of shorter duration, and (5) that warrantless video surveillance ought to be prohibited even when one of the parties consents to it).

250. Electronic Surveillance Standards, *supra* note 7, Standard 2-5.8(I).

251. *See* 18 U.S.C. § 2518(5) (1994) (stating that electronic surveillance "shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter").

prohibition.[252] Are these provisions sufficient for accomplishing minimization of video surveillance or should they be more detailed for *both* aural and video surveillance (i.e., by requiring termination of surveillance when no one reasonably suspected of criminal activity is being surveilled, and allowing only spot checks thereafter)?

Finally, both the Electronic Surveillance Standards and federal law exempt from regulation the interception of communications involving a party who has consented to the interception.[253] As applied to video surveillance, on its face this provision's requirement that the consenting party be present during the surveillance prohibits the use of a "teddy bear camera" to observe a babysitter while the parents are gone. Moreover, this provision requires termination of warrantless video surveillance if the consenter leaves the room during a transaction. At the same time, eliminating the presence requirement might allow the owner of a house to authorize surveillance of the activities of guests which he or she does not personally observe. Even guests have expectations of privacy that should be considered reasonable, especially when, for instance, they are alone in a guest room or reasonably assume the owner has left the premises.[254]

14. To What Extent Should the Public Be Involved in Authorizing Video Surveillance of the Public?

Several members of the Task Force wondered whether involving the public in the implementation of long-term video surveillance of public areas (and detection device checkpoints) was necessary given the fact that politically accountable officials are already involved in the decision. The Task Force decided that although this latter input might be sufficient in many instances, the public should be given the opportunity to register its views. Both from philosophical and practical standpoints, government searches that affect large groups of people should be mediated through the public process.[255] Involvement of the public affected by the

252. *See* Scott v. United States, 436 U.S. 128, 138-39 (1978) (holding that a bad faith failure to minimize does not violate the statute because the focus should be "on agents' actions not their motives").

253. *See* Electronic Surveillance Standards, *supra* note 7, Standard 2-5.1; 18 U.S.C. § 2511(2)(c)-(d) (1994).

254. At least one court has held that even the *presence* of a consenting party during surveillance does not vitiate Fourth Amendment protection. *See* United States v. Shabazz, 883 F. Supp. 422 (D. Minn. 1995) (holding that warrantless audio and video surveillance of a suspect's room violates the Fourth Amendment even though conducted only while a consenting informant is in the room).

255. *Cf.* William Stuntz, *Implicit Bargains, Government Power, and the Fourth Amendment*, 44 STAN. L. REV. 553, 588-89 (1992) (arguing that cases like *Martinez-Fuerte* and *Sitz*, which leave checkpoints to departmental discretion, nonetheless seem to suggest

surveillance can act as a check on elitist decision-making, provide useful information as to the scope of the problem, encourage a sense of community involvement, and diminish the discomfort associated with the surveillance by increasing understanding of its nature and purpose.

On the other hand, the Task Force rejected the suggestion that the public be permitted to "veto" particular video surveillance.[256] Such a provision was deemed both unworkable and unnecessary. Determining when the public had "vetoed" surveillance would be difficult; at the same time, overwhelming public aversion to particular cameras would presumably persuade the police department and city council to back down without formally gauging whether a veto has taken place.[257]

A related issue concerns what the public should be told about proposed video surveillance. Some members of the Task Force believed that the precise capabilities of the cameras, including magnification and audio capability, ought to be disclosed. Other members, echoing the arguments against periodic public dissemination of specific physical surveillance information,[258] argued for a less revelatory approach. The Task Force ultimately concluded that the public should be informed of the "intended location and general capability of the camera."[259] By using the words "general capability," the standard conveys that not every technical aspect of the camera need be disclosed to the public.

---

that where group stops are involved "politics provides an adequate remedy for overzealous police action; groups . . . unlike the solitary suspect, can protect themselves from overzealous police tactics at the polls").

256. *See* Jennifer Granholm, *Video Surveillance on Public Streets: The Constitutionality of Invisible Citizen Searches*, 64 U. DET. L. REV. 687, 711 (1987).

257. In some jurisdictions, video cameras have been removed after public outcry. Associated Press, *Spying Fears Get Cameras Removed*, GAINESVILLE SUN, June 20, 1996, at 1B (reporting that five cameras being used to monitor traffic were removed); Barbara Yaffe, *Ontario Zaps Big Brother's Photo Radar*, EDMONTON J., June 24, 1995, at C3 (reporting that citizens voted for a local politician who promised to remove "the government eyeball on provincial roadways"). To some extent, the hostility in these cases may have stemmed from the fact that the cameras effectively caught speeders.

258. *See supra* text accompanying notes 232-33.

259. *See* Standard 2-6.3(b)(ii)(A), *infra* Appendix.

E. Tracking Devices

15. When Is Probable Cause Required for Tracking?

Legal regulation of tracking devices is derived largely from two Supreme Court cases briefly described earlier.[260] In *United States v. Knotts*,[261] the Supreme Court held that using a beeper to track a car through public streets is not a search under the Fourth Amendment. According to the Court, it is not reasonable to expect privacy with respect to one's route or destination when traveling on the roadways.[262] In contrast, in *United States v. Karo*,[263] the Court held that the use of a beeper to locate an item inside a particular house *is* a search, and that judicial authorization for such a search is required. However, the warrant need not state with particularity the place to be "searched" by the beeper when, as will usually be the case, that place is unknown.[264] Further, the Court left open whether reasonable suspicion (as opposed to probable cause) is sufficient to authorize the warrant.[265]

Despite objections from law enforcement organizations, the Task Force opted for the probable cause standard whenever a tracking device is used to locate an item or person within a private location.[266] The intimation of *Karo* notwithstanding, the Court has firmly stated in other contexts that a Fourth Amendment search outside of the weapon frisk and "special needs" scenarios requires probable cause.[267] In this

---

260. *See supra* text accompanying notes 26-29. Title III mentions tracking devices, but does not seriously regulate them, merely providing that "[i]f a court is empowered to issue a warrant or other order for the installation of a mobile tracking device, such order may authorize the use of that device within the jurisdiction of the court, and outside that jurisdiction if the device is installed in that jurisdiction." 18 U.S.C. § 3117(a) (Supp. 1996). This provision allows beepers authorized in one jurisdiction to be used in other jurisdictions.

261. 460 U.S. 276 (1983).

262. *See id.* at 282.

263. 468 U.S. 705 (1984).

264. *See id.* at 718.

265. *See id.* at 718 n.5.

266. Note that the word "location" is used in the standard, rather than the word "place." As defined in Standard 2-6.2(f), a private place is one which, if entered physically, would be entitled to a constitutionally protected reasonable expectation of privacy. It is possible that various locations within such a place are not protected by the Fourth Amendment when viewed from the outside, without a physical intrusion. Indeed, this possibility is recognized in *Karo*, when the Court states that the use of a beeper to see a container is the equivalent of an entry only if the government "employs an electronic device to obtain information that it could not have obtained by observation from outside the curtilage of the house." 468 U.S. at 715.

267. Whereas a frisk for weapons only requires reasonable suspicion, see Terry v. Ohio, 392 U.S. 1, 20 (1968), and a special needs search (e.g., an administrative or regulatory search) need only be "reasonable" under the circumstances, see New Jersey v. T.L.O., 469

situation, the tracking device functions like a device that sees through walls, because it allows the police to determine precisely where an item is and, by inference, where the person who carried the item is. The Task Force concluded that such an intrusion necessitates justification at the probable cause level.

Although the standard also provides that public tracking need only meet the legitimate objective test,[268] the practical impact of this standard is that probable cause will usually be required for long-term tracking.[269] Several factors mitigate the burden on law enforcement in that regard, however. First, precisely because the destinations of the device are not known, probable cause here focuses solely on the likelihood that evidence will be discovered; as *Karo* indicates, the place ultimately to be searched need not be stated with particularity. Second, if the device is installed in an illicit item (such as a bale of marijuana or a car that is later stolen), such probable cause will generally readily be found because, once acquired, possession of the item is a crime.[270] Third, paragraph (c) sets out an exigency exception to the court order requirement, which applies whenever there is insufficient time to obtain a warrant. Finally, under provision (b)(i), if a person agrees to be "bugged," a consent exception to the warrant and suspicion requirements exists.

U.S. 325 (1985) (search of student's purse), a typical search requires probable cause. *See, e.g.*, Arizona v. Hicks, 480 U.S. 321, 328-29 (1987) (holding that probable cause is required to view serial numbers on a stereo and specifically rejecting a reasonable suspicion standard for "cursory" searches); Ybarra v. Illinois, 444 U.S. 85, 90-94 (1979) (holding that probable cause is required to search a person unless there is present danger).

268. *See* Standard 2-6.4(b)(ii), *infra* Appendix. Some members of the Task Force, echoing several commentators, contended that reasonable suspicion was the appropriate standard in this context. They argued that public tracking infringes privacy, the interest in anonymity, and freedom of travel, in a way that typical naked-eye viewing does not — it allows continuous long-term monitoring of the particular routes traveled; the starting, stopping, and intermediate points of the travel; and the contents of one's car or suitcase. *See* McAdams, *supra* note 232, at 311 ("because [without a beeper] the combination of these elements will be unknown to any single person in almost every case, the driver's privacy remains secure"); Wayne R. LaFave, *Nine Key Decisions Expand Authority to Search and Seize*, 69 A.B.A. J. 1740, 1740 (1983) (noting that in cases where there is no surveillance, "only an army of bystanders, conveniently strung out on the route and who not only 'wanted to look' but also wanted to pass on what they observed to the next in line" would truly invade the driver's privacy interest and expectations). The Task Force also noted that this type of physical surveillance is more intrusive than other types of covert surveillance of public activity (e.g., using video cameras, telescopic, or illumination devices); the latter types of surveillance are usually relatively brief and in any event focus on one particular area.

269. *See supra* text accompanying notes 165-67.

270. *Cf.* CLIFFORD S. FISHMAN & ANNE T. MCKENNA, WIRETAPPING & EAVESDROPPING § 28.10 (2d ed. 1995) (noting that tracking devices placed in packages mailed from overseas containing contraband require no warrant).

16. Duration of the Court Order

Under Title III, a wiretap order is valid for thirty days.[271] An early version of the standards set this time limit on tracking orders as well.[272] However, many knowledgeable members of the Task Force claimed that such a limitation on the use of beepers and other tracking devices would be impractical in this context. For instance, in an effort to ferret out the identity and location of as many members of a drug ring as possible, tracking often might continue over months or even years. Thirty days was therefore seen as unreasonably short.

Yet as several courts have recognized,[273] and as *Karo* itself indicates,[274] without some limitation, tracking surveillance becomes an extreme intrusion, potentially amounting to weeks of surveillance apparently justified solely by the mere hope that useful information will be produced. The time period ultimately chosen (sixty days) is identical to the durational limitations on court orders for "pen registers" under Title III.[275] Because of the great likelihood that a tracked item will end up in a private location during an extended period, an officer contemplating using a tracking device in this situation would be well-advised to seek a warrant, with its attendant durational limitation.

F. Illumination and Telescopic Devices

17. The Confirmation Exception

Some courts have permitted the use of telescopic and illumination devices to observe the inside of a house if an inadvertent naked-eye sighting gives police reasonable suspicion that criminal activity is taking place and the enhanced surveillance is necessary to confirm that suspicion.[276] This "confirmation" exception to the usual probable cause

---

271. *See* 18 U.S.C. § 2518(5) (1994).

272. *See* Standard 2-6.4(c) (draft of Feb. 10, 1997) (on file with the *Harvard Journal of Law and Technology*).

273. *See, e.g.*, United States v. Butts, 710 F.2d 1139, 1149 (5th Cir. 1983); United States v. Cofer, 444 F. Supp. 146, 151 (W.D. Tex. 1978); *Cf.* United States v. Long, 674 F.2d 848, 852 (11th Cir. 1982) (holding that a warrant that allows beeper use for ninety days is permissible if the beeper is only used for seven days).

274. According to *Karo*, to obtain a warrant for a tracking device the government must identify the object into which the beeper is to be placed, explain the circumstances justifying installation of the beeper, *and* state the length of time it is required. United States v. Karo, 468 U.S. 708, 718 (1984).

275. *See* 18 U.S.C. § 3123(c)(1) (Supp. 1996). A pen register records numbers dialed on a telephone without overhearing verbal communications. Its use is not a Fourth Amendment search. *See* Smith v. Maryland, 442 U.S. 735, 745-46 (1979).

276. *See supra* note 62.

requirement could arguably be justified by the need to immediately confirm or dispel the suspicion of criminal activity. Such a situation might occur, for instance, if an officer on the street sees what looks like a drug deal taking place in a second story window and uses binoculars or a nightscope to verify or dispel the suspicion.

One version of Standard 2-6.5 recognized this exception if "the observation is from a lawful vantage point, of brief duration, and focuses solely on the area necessary to confirm reasonable suspicion acquired from that vantage point that evidence of crime will thereby be discovered."[277] Ultimately, however, the Task Force deleted this provision. In the usual confirmation situation, the activity or condition observed with the enhancement device will be legitimately observable on *no* suspicion (at least as far as the Fourth Amendment is concerned) because it is not "private." For instance, using binoculars to confirm the naked-eye sighting in the foregoing example would generally not constitute a search, because the subjects are observable through a window. In situations where this is not the case, the danger is that the exception will permit intrusive surveillance on less than probable cause, in contravention of the Fourth Amendment. For instance, under this exception, a tip providing reasonable suspicion that gambling is currently taking place in a particular house could be said to give the police authority to use a telescopic device to look at documents inside the house and determine whether they are racing forms.[278] The Task Force decided that the traditional warrant/exigent circumstances formulation adequately balanced law enforcement and privacy interests in this context.

G. Detection Devices

18. Are Heat Waves "Abandoned"?

Because general detection devices reveal more than just contraband or weapons, Standard 2-6.6(a) requires that their use be justified by probable cause or one of the well-recognized exceptions to the probable cause standard.[279] Probably the most controversial use of detection devices aimed at private places is thermal imaging, which permits law enforcement officials to identify heat sources within a building, and thus facilitates location of drug laboratories or in-house marijuana farms. A

---

277. *See* Standard 2-6.5(a)(iii) (draft of Feb. 10, 1997) (on file with the *Harvard Journal of Law and Technology*).

278. *But cf.* United States v. Kim, 415 F. Supp. 1252 (D. Haw. 1976) (holding that the use of a telescope to observe illegal gambling, including reading material, inside a high rise apartment requires probable cause).

279. *See supra* note 168 and accompanying text.

majority of courts have held, and some members of the Task Force argued, that the use of such a device to determine the heat output of a private place is not a search, because it merely detects heat "waste" that has been "abandoned" by the house occupant.[280]

The Task Force ultimately adopted the contrary position, persuaded by the Tenth Circuit's initial reasoning on this issue.[281] As that court indicated, heat waves that emanate through the walls of a house are similar to the sound waves picked up by a microphone.[282] In both instances, it is the *source* of the waves, not the "abandoned" waves, that interests the police. Further, because even relatively primitive thermal imaging devices can resolve heat differentials as small as one-half of a degree,[283] they have the potential for discerning a variety of activities associated with an expectation of privacy.

19. Are General Detection Devices Too General?

It could be argued that the use of general detection devices should always require probable cause (even if a recognized exception to probable cause exists) because they often reveal more than would a traditional, legitimate physical search. To illustrate, suppose the police have grounds to frisk a suspect or search the immediate premises surrounding an arrestee based on a reasonable suspicion of danger. A detection device that can "see" into containers might easily reveal more than a traditional search in these situations.[284]

Although no Task Force members took the position that the use of general detection devices should always require probable cause, several

---

280. Some of these courts also analogize thermal imaging to the use of a dog to detect drugs, which the Supreme Court indicated is not a search in *United States v. Place*, 462 U.S. 696, 707 (1983). *See, e.g.*, United States v. Pinson, 24 F.3d 1056, 1058 (8th Cir. 1994). However, thermal imaging is clearly not a contraband-specific technique, and thus *Place* is inapposite here.

281. *See* United States v. Cusumano, 67 F.3d 1497 (10th Cir. 1995), *vacated*, 83 F.3d 1247 (10th Cir. 1996). On rehearing en banc, the court held that there was probable cause for the warrant that eventually issued, absent any consideration of the thermal imaging, and refused to reach the issue of whether the use of the thermal imaging constituted a search. Cusumano, 83 F.3d at 1250.

282. *See id.* at 1502.

283. *See* Matthew L. Zabel, *A High-Tech Assault on the "Castle": Warrantless Thermal Surveillance of Private Residences and the Fourth Amendment*, 90 NW. U. L. REV. 267, 269 (1995).

284. For example, in *Terry v. Ohio*, 392 U.S. 1 (1968), the Supreme Court suggested that an officer can pat down the outer clothing but should generally not reach into pockets or beneath garments unless a weapon-like item is felt. *Id.* at 29-30. In practice, however, a frisk is likely to be much more intrusive. *See* JONATHAN RUBINSTEIN, CITY POLICE 310-11 (1973) (describing the probing nature of the typical frisk taught at police academies).

expressed concern about the potential for "overbroad" searches. The detection device standard nonetheless incorporates all of the traditional exceptions to the probable cause requirement for three reasons.[285] First, the use of a detection device permits the officer to remain a safer distance from the suspect. Second, it avoids the need for highly intrusive placement of hands over the suspect's entire body. Third, it identifies weapons and other items with greater certainty and locates them with greater precision. Thus, post-frisk searches into clothing will be fewer in number and more limited in scope. Similarly, in home entry situations, the use of detection devices might dissipate the fear of danger, so that "no-knock" entries will become unnecessary. In protective sweep situations, detection devices will give the officer a more definite reading concerning others on the premises and will decrease the chances of a dangerous surprise confrontation.

Nonetheless, it remains possible that the use of general detection devices in these situations could disclose more private information than the typical search or frisk, especially when the devices supply images rather than simply detect characteristics of items. In recognition of this fact, the Standards Committee added the provision that procedures should be adopted "to ensure that the capabilities of any device used conform as closely as possible to the authorized objective or objectives of the surveillance."[286] This provision means that if the police must use a general detection device, they should use one that will achieve their objective with as little revelation of other material as possible.[287]

20. Should Specific Devices Be Immune from Regulation?

Conversely, the issue of whether there should be *any* limitations on contraband- or weapon-specific devices was also debated. Some members of the Task Force felt that police should be able to aim a device that detects only weapons at anyone they choose, based on the intimation in *United States v. Place*[288] that if a device detects only contraband its use entails no search because it discovers nothing of private significance.[289] The Task Force ultimately rejected this stance because of the fact that in many states a weapon is not contraband.[290] Instead the Task Force distinguished between weapon-specific and contraband-

285. *See* Standard 2-6.6(a)(ii)-(iii), *infra* Appendix.

286. *See* Standard 2-6.6(d)(iii), *infra* Appendix.

287. *See supra* text accompanying note 178. For an argument against the approach endorsed by the standards and in favor of a reasonable suspicion requirement for use of detection devices in non-checkpoint situations, see Harris, *supra* note 119.

288. 462 U.S. 696 (1983).

289. *See id.* at 707.

290. *See supra* note 141 and accompanying text.

specific devices, to allow the use of the former whenever police may validly look for weapons (e.g., in frisk situations) but to prevent their random, suspicionless use except when weapons are in fact contraband (as in airports or in jurisdictions that make carrying a concealed weapon a crime).[291]

A related argument, made by a sizeable segment of the Task Force, was that if a device is truly contraband-specific its use should never require justification. The case for this position is especially strong if the device is deployed surreptitiously and relies on technology that causes no physical or other harm. However, the group ultimately decided that when surveillance is of the home the use of such a device generally should require probable cause.[292] The Task Force concluded that at least one place of ultimate repose should be maintained, sacrosanct from suspicionless invasion regardless of the precision that technology affords.[293] Some members may also have been influenced by the reality that devices that can see through walls are unlikely to detect *only* contraband and that, even if they did, they could easily be used in a discriminatory fashion that would be particularly repugnant when aimed at the home.

21. Fixed Checkpoints and Compelling Government Interests

The Supreme Court has upheld the use of checkpoints to address significant crime problems like illegal immigration[294] and drunk driving.[295] This fact, combined with the relatively nonintrusive nature of detection devices (i.e., the fact that they allow police to avoid physical touching), led several members of the Task Force to argue that fixed checkpoints using detection devices should be permissible upon a relatively meager showing of need. So, for example, if a neighborhood is experiencing a surge in violent crime, police should be able to set up detection device checkpoints to detect and deter the importation of weapons into the neighborhood.

While not fully addressing the propriety of such usage, the language adopted by the Task Force clearly imposes more stringent limitations on

---

291. *See* Standard 2-6.6(b)-(c), *infra* Appendix.

292. *See* Standard 2-6.6(a)-(b), *infra* Appendix.

293. *Cf.* Michael Adler, *Cyberspace, General Searches, and Digital Contraband: The Fourth Amendment and the Net-Wide Search*, 105 YALE L.J. 1093, 1120 (1996) (arguing against suspicionless "surgical" searches of computers designed to obtain only information about illegal activity on the ground that "[t]he values of one's home and office as a psychological refuge and as a source of power independent of the government represent a pair of interests protected by the property-model of the Fourth Amendment").

294. *See* United States v. Martinez-Fuerte, 428 U.S. 543 (1976).

295. *See* Michigan Dep't of State Police v. Sitz, 496 U.S. 444 (1990).

checkpoints than does Supreme Court case law. Not only does Standard 2-6.6(a)(iv) require the involvement of politically accountable officials (a requirement arguably dictated by the Court's decisions),[296] it also requires that the public affected by the checkpoint be involved in the decision (which is clearly not mandated by Court rulings). Additionally the standard requires a finding that the checkpoint serve "a *compelling* government interest that no contraband pass by that checkpoint" or "a *compelling* government interest that no weapons pass by that checkpoint into a place where the presence of weapons would be *extraordinarily* hazardous."[297] Use of the word "compelling" in these provisions conveys a requirement that the checkpoint be the least intrusive, effective way of achieving a government aim of great magnitude, as with checkpoints at prisons, borders, court buildings, and airports. The Task Force concluded that such language was necessary because checkpoints usually involve a seizure of some sort, often of large numbers of people, and because aiming a detection device at individuals is still likely to be perceived as intrusive, especially when its necessity is not clear.

Returning to the neighborhood weapon detection checkpoint scenario, establishing such checkpoints on public streets would seldom be permissible under this standard, even taking into account the fact that the use of a general detection device would facilitate the checkpoint's purpose by less intrusive and embarrassing means than conventionally used. The practice of subjecting everyone seeking to enter a particular street or residential area to a contraband check is repugnant for several reasons. First, unlike the four contexts mentioned in the previous paragraph — where checkpoints do not stigmatize anyone because the practices have been so long accepted and do not discriminate between different segments of society — checkpoints on public roads could taint both the area sealed off and those who enter it. Second, such checkpoints would hamper the freedom to travel, which is not an issue in the context of prisons and public buildings, and which already occurs at airports and at the border given the need for documentation checks. Third, the use of such checkpoints could create an atmosphere of oppression, precisely because it could be equated with prison, border, and airport situations.

---

296. *See supra* note 221.

297. Standard 2-6.6(a)(iv), *infra* Appendix (emphasis added). Standard 2-6.6(a)(iv)(C) lays out somewhat different requirements for temporary checkpoints. *See supra* text accompanying note 169.

V. CONCLUSION

As the name implies, the American Bar Association's Tentative Draft Standards Concerning Technologically-Assisted Physical Surveillance is a work in progress. Comments on the foregoing material are encouraged. Final approval by the ABA hierarchy is still some time away,[298] so feedback could have an impact. Indeed, it is anticipated that the content of at least some of the standards will change prior to their submission to the House of Delegates.

At the same time, if it has done nothing else, the work of the Task Force on Technology and Law Enforcement has persuasively demonstrated that some regulatory structure governing the use of physical surveillance technology is necessary. This work provides a model for future attempts to establish guidelines for other types of surveillance, and for search and seizure regulation generally.

298. As noted earlier, *supra* note 14, the review process leading to ABA House of Delegates approval is multi-layered, including two "readings" by the Criminal Justice Section Council. The first reading will take place in August, 1997. A second reading must take place before the standards can be forwarded to the House of Delegates.

APPENDIX:
ABA TASK FORCE ON TECHNOLOGY AND LAW ENFORCEMENT

TENTATIVE DRAFT STANDARDS CONCERNING TECHNOLOGICALLY-ASSISTED PHYSICAL SURVEILLANCE

As revised after meeting with
Criminal Justice Standards Committee
February 24, 1997

Standard 2-6.1. General Principles

(a) *Need for Surveillance.* Technologically-assisted physical surveillance can be an important law enforcement tool. It can facilitate the detection, investigation, prevention and deterrence of crime, the safety of officers and citizens, the apprehension and prosecution of criminals, and the protection of the innocent.

(b) *Need for Regulation.* Law enforcement use of technologically-assisted physical surveillance can also diminish privacy, freedom of speech, association and travel, and the openness of society. It thus may need to be regulated.

(c) *Factors Relevant to Regulating Use of Surveillance.* Whether technologically-assisted physical surveillance should be regulated and, if so, to what extent should be determined by the following factors:

(i) the law enforcement interests implicated by the surveillance, including:

(A) the nature of the law enforcement objective or objectives sought to be achieved;

(B) the extent to which the surveillance will achieve the law enforcement objective or objectives; and

(C) the nature and extent of the crime involved;

(ii) the extent to which the surveillance technique invades privacy, which should include consideration of:

(A) the nature of the place, activity, condition or location to be surveilled;

(B) the care that has been taken to enhance the privacy of such place, activity, condition, or location;

(C) the lawfulness of the vantage point, including whether either the surveillance or installation of surveillance equipment requires a physical intrusion;

(D) the availability and sophistication of the surveillance technology;

(E) the extent to which the surveillance technology enhances the law enforcement officer's natural senses;

(F) the extent to which the surveillance of subjects is minimized in time and space;

(G) the extent to which the surveillance of non-subjects is likewise minimized; and

(H) whether the surveillance is covert or overt;

(iii) the extent to which the surveillance diminishes or enhances the exercise of First Amendment freedoms and related values; and

(iv) the extent to which the surveillance technique is less intrusive than other available effective and efficient alternatives.

(d) *Implementation of the Surveillance.* Officers conducting regulated technologically-assisted physical surveillance should be governed by the following considerations:

(i) The subjects of the surveillance should not be selected in an arbitrary or discriminatory manner.

(ii) The scope of the surveillance should be limited to its authorized objectives and be terminated when those objectives are achieved.

(iii) The particular surveillance technique should be capable of doing what it purports to do and be used solely by officers trained in its use.

(iv) When a particular surveillance device makes use of more than one regulated technology and the technologies are governed by differing rules, the more restrictive rules should apply.

(v) Reasonable notice of the surveillance should be given at an appropriate time and in an effective manner.

(vi) Disclosure and use by law enforcement officers of information obtained by the surveillance should be permitted only for designated lawful purposes.

(vii) Protocols should be developed for the maintenance and disposition of surveillance records not required to be maintained by law.

(e) Rule-making and Decision-making Entities. A variety of entities, including the courts, legislatures, executive officials, prosecutors, law enforcement agencies, and the public, have a responsibility in assessing how best to regulate the use of technologically-assisted physical surveillance. The role that each should play in formulating, monitoring and enforcing regulatory requirements depends on such factors as the:

(i) legal basis for the regulation;

(ii) invasiveness and urgency of the surveillance;

(iii) need for deference to expertise in law enforcement;

(iv) extent to which local conditions vary;

(v) value of sharing decisionmaking; and

(vi) number of people and size of the geographic area affected by the surveillance.

(f) *Accountability and Control.* Government officials should be held accountable for use of regulated technologically-assisted physical surveillance technology by means of:

(i) administrative rules which ensure that the information necessary for such accountability is maintained;

(ii) in addition to any exclusionary sanction mandated by the Fourth Amendment or legislation, appropriate administrative sanctions when rules promulgated pursuant to Standard 2-6.1(g) regarding use of technologically-assisted physical surveillance are violated;

(iii) periodic review by law enforcement agencies of the scope and effectiveness of technologically-assisted physical surveillance; and

(iv) public dissemination of information about the general type or types of surveillance being used and the frequency of their use.

(g) *Written Guidance to Law Enforcement Officers.* Each law enforcement agency should develop written instructions regarding resort to regulated technologically-assisted physical surveillance and should mandate that officers of that agency comply with those instructions. These instructions should include:

(i) the requirements as to specific types of surveillance, as set out in Standards 2-6.3 through 2-6.6;

(ii) the rules developed by other agencies pursuant to Standard 2-6.1(e); and

(iii) such other rules as are necessary to implement these general principles in specific contexts.

Standard 2-6.2. Definitions

The following definitions apply to Standards 2-6.3 through 2-6.6.

(a) *Covert surveillance.* Surveillance intended to be concealed from any subject of the surveillance.

(b) *Detection devices.* Devices used to detect the presence of a particular object (e.g., explosives, drugs, weapons, or certain chemicals) or characteristic (e.g., shape, size, density, hardness, material, texture, temperature, scent) that is concealed behind

opaque inanimate barriers. Such a device is of the *contraband-specific* type if it can only reveal the presence of an object which it is always or virtually always criminal to possess or use in the existing circumstances. Such a device is *weapon-specific* if it can only reveal the presence of a weapon.

(c) *Illumination devices.* Devices that make visible details not visible to the naked eye because of poor lighting conditions.

(d) *Legitimate law enforcement objective.* Detection, investigation, deterrence or prevention of crime, protection from harm, or apprehension and prosecution of a suspected criminal. An action by a law enforcement officer is "reasonably likely to achieve a legitimate law enforcement objective" if there are articulable reasons for concluding that one of these objectives may be met by taking the action.

(e) *Overt surveillance.* Surveillance of which a reasonable person would be aware.

(f) *Private.* An activity, condition or location is private when the place where it occurs or exists and other relevant considerations, such as those listed in Standard 2-6.1(c)(ii), afford it a constitutionally protected reasonable expectation of privacy. A *place* is private if physical entry therein would be an intrusion upon a constitutionally protected reasonable expectation of privacy.

(g) *Reviewing law enforcement official.* A law enforcement officer other than the person who will implement the surveillance. Such an officer may be *supervisory* (e.g., a sergeant, lieutenant or commander of a district or unit), or *politically accountable* (e.g., a department head or a prosecutor). A supervisory officer should have participated in specialized training on surveillance techniques and applicable legal guidelines.

(h) *Telescopic devices.* Devices that make visible details not visible to the naked eye because of distance.

(i) *Tracking devices.* Devices used to track movement of persons, effects, or vehicles such as beepers, over-the-horizon radar, and Intelligent Transportation Systems.

(j) *Video surveillance.* Use of a lawfully positioned camera as a means of viewing or recording activities or conditions other than those occurring within the sight or immediate vicinity of a law enforcement official (or agent thereof) who is aware of such use.

Standard 2-6.3. Video surveillance

(a) Video surveillance of a private activity or condition is permissible when it complies with provisions applicable to electronic interception of communications [see Standards 2-___* of this Chapter], as modified for video surveillance.

(b) Overt video surveillance for a protracted period not governed by Standard 2-6.3(a) is permissible when:

(i) a politically accountable law enforcement official or the relevant politically accountable governmental authority concludes that it will:

(A) not view a private activity or condition; and

(B) will be reasonably likely to achieve a legitimate law enforcement objective; and

(ii) the public to be affected by the surveillance:

(A) is notified of the intended location and general capability of the camera; and

(B) has the opportunity, both prior to the initiation of the surveillance and periodically during it, to express its views of the surveillance and propose changes in its execution, through a hearing or some other appropriate means.

(c) All video surveillance not governed by Standard 2-6.3(a) or (b) is permissible when a supervisory law enforcement official, or the surveilling officer when there are exigent circumstances, concludes that the surveillance:

---

* This provision is subject to change, depending upon the Task Force's proposals concerning communications surveillance.

(i) will not view a private activity or condition; and

(ii) will be reasonably likely to achieve a legitimate law enforcement objective.

Standard 2-6.4. Tracking Devices

(a) Installation of a tracking device other than as part of a systemwide program authorized by the legislature is permissible:

(i) if installation involves entering a private place without consent, only when there is probable cause to believe that:

(A) the object to be tracked is at the location to be entered; and

(B) subsequent monitoring of the device will reveal evidence of crime; and

(ii) in all other cases, when subsequent monitoring of the device is reasonably likely to achieve a legitimate law enforcement objective.

(b) Monitoring of a tracking device is permissible:

(i) to determine whether or where the device is located within a particular private location, only when there is probable cause to believe that such monitoring will reveal evidence of crime, provided that, if one or more of the subjects of the monitoring consent to have the tracking device accompany their persons, the monitoring need only be reasonably likely to achieve a legitimate law enforcement objective; and

(ii) in all other cases, only so long as there continues to be a reasonable likelihood that such monitoring will achieve a legitimate law enforcement objective,

(c) Installation pursuant to paragraph (a)(i) and nonconsensual monitoring pursuant to paragraph (b)(i) shall be permitted only on written authorization by a judicial officer, except when obtaining the required court order is not feasible due to exigent

circumstances, in which case an order should be sought as soon as practicable. The court order should authorize surveillance for as long as necessary to achieve the authorized objective(s) of the surveillance, limited to a maximum of 60 days absent articulable facts demonstrating a need for longer surveillance. Extensions of 60 days should be permitted on reauthorization by a judge under the appropriate standard.

Standard 2-6.5. Illumination and Telescopic Devices

(a) Use of an illumination or telescopic device to observe a private activity or condition is permissible when:

(i) a judicial officer has issued a warrant on probable cause to believe evidence of crime will thereby be discovered; or

(ii) obtaining a warrant is not feasible due to exigent circumstances, and the surveilling officer has probable cause to believe evidence of crime will thereby be discovered.

(b) Use of an illumination or telescopic device that is not governed by Standard 2-6.5(a) is permissible when:

(i) the use is overt and not prolonged with respect to any given area; or

(ii) it is reasonably likely to achieve a legitimate law enforcement objective.

Standard 2-6.6. Detection Devices

(a) Use of a detection device to search a private place (whether associated with a person, premises, or effect) is permissible when:

(i) the search is on probable cause:

(A) pursuant to a search warrant issued by a judicial officer; or

(B) without a search warrant when obtaining such a warrant:

(1) would not be feasible due to exigent circumstances; or

(2) is unnecessary because of the lesser expectation of privacy associated with the private place; or

(ii) the device is directed only at places the police are authorized to search:

(A) incident to a lawful custodial arrest;

(B) with the consent of a person with real or apparent authority to give such consent; or

(C) pursuant to a lawful inventory; or

(iii) upon grounds for such protective action, the device is directed only at places the police are authorized to:

(A) subject to a protective frisk;

(B) otherwise enter without notice in the interest of self-protection; or

(C) subject to a protective sweep; or

(iv) the device is directed only at persons or effects passing a checkpoint, if:

(A) the checkpoint is fixed and has been established to serve a compelling government interest that no contraband pass by that checkpoint, as determined by an appropriate politically accountable law enforcement official or governmental authority;

(B) the checkpoint is fixed and has been established to serve a compelling government interest that no weapons pass by that checkpoint into a place where the presence of weapons would be extraordinarily hazardous, as determined by an appropriate politically accountable law enforcement official or governmental authority; or

(C) the checkpoint is temporary and has been established in response to a substantial risk of death or serious bodily harm, upon a finding made of record by a supervisory law enforcement official that:

(1) there is a reasonable suspicion that the instrumentality threatening such harm or the person or persons threatened will thereby be discovered; and

(2) the anticipated size of the group of persons involved is reasonable in light of the purpose for which the device is to be used; and

(D) with respect to the checkpoints in (A) and (B), the public to be affected by the checkpoint:

(1) is notified of the intended location of the checkpoint; and

(2) has the opportunity, both prior to the initiation of the surveillance and periodically during it, to express its views about the checkpoint and propose changes in its execution, through a hearing or some other appropriate means.

(b) Use of a contraband-specific detection device to search a private place in circumstances other than those authorized by Standard 2-6.6(a) is permissible if it does not involve search of a place of residence and:

(i) such use is reasonably likely to achieve a legitimate law enforcement objective; and

(ii) if a seizure is made to facilitate such use, there are grounds for the seizure.

(c) Use of a weapon-specific detection device is permissible in the circumstances specified in Standard 2-6.6(a)(iii), even absent any individualized suspicion of danger that otherwise would be required.

(d) Law enforcement agencies using detection devices should adopt procedures:

(i) to avoid disclosure of gender-specific anatomical features to officers of the opposite gender; and

(ii) to ensure that no physical harm is caused by such devices; and

(iii) to ensure that the capabilities of any device used conform as closely as possible to the authorized objective or objectives of the surveillance.