ABA Standards for Criminal Justice
Electronic Surveillance
Third Edition
Section B: Technologically-Assisted Physical Surveillance

Copyright © 1999 by the American Bar Association

All rights reserved. No part of this book may be reproduced in any form or by any electronic or mechanical means including information storage and retrieval systems without permission in writing from the publisher, except by a reviewer who may quote brief passages in a review or for non-commercial educational or training use provided proper attribution is given to the American Bar Association.

Library of Congress Catalog Card No. 99-73289
ISBN-1-57073-711-8

The commentary contained herein does not necessarily represent the official position of the ABA. Only the text of the black-letter standards has been formally approved by the ABA House of Delegates as official policy. The commentary, although unofficial, serves as a useful explanation of the black-letter standards.

Project of the
American Bar Association
Criminal Justice Standards Committee
Criminal Justice Section
740 Fifteenth Street, NW
Washington, D.C. 20005
202/662-1500

Printed in the United States of America

ABA Standards for Criminal Justice
Electronic Surveillance
Third Edition
Section B: Technologically-Assisted Physical Surveillance

Niki Kuckes, Chairperson
Criminal Justice Standards Committee 1998-1999
Charles R. English
Chairperson, Criminal Justice Standards Committee 1997-1998
Michael Th. Johnson
Chairperson, Criminal Justice Standards Committee 1996-1997
Irma S. Raker
Chairperson, Criminal Justice Standards Committee 1995-1996
William H. Jeffress, Jr.
Chairperson, Criminal Justice Standards Committee 1994-1995
Sheldon Krantz
Chairperson, Criminal Justice Standards Task Force on Technology and Law Enforcement
Myrna Raeder
Chairperson, ABA Section of Criminal Justice 1998-1999
Ronald Goldstock
Chairperson, ABA Section of Criminal Justice 1997-1998
William W. Taylor, III
Chairperson, ABA Section of Criminal Justice 1996-1997
Cara Lee T. Neville
Chairperson, ABA Section of Criminal Justice 1995-1996
E. Michael McCann
Chairperson, ABA Section of Criminal Justice 1994-1995

Liaisons to the Criminal Justice Standards Committee

Herbert B. Dixon, Jr.
ABA Judicial Division
Kathleen A. Felton
U.S. Department of Justice
William A. Helm
National Association of Attorneys General
Albert J. Krieger
National Association of Criminal Defense Lawyers
Norman K. Maleng
National District Attorneys Association
Robert E. Shepherd, Jr.
ABA Juvenile Justice Center
Neal R. Sonnett
ABA Criminal Justice Section Council
Scott Wallace
National Legal Aid and Defender Association

July 1999

Staff to the Criminal Justice Standards Committee

Susan W. Hillenbrand
Project Director
Aaron Sheppard
Project Assistant

During the preparation of the Technologically-Assisted Physical Surveillance Standards, the following also served on the Criminal Justice Standards Committee: John M. Burkoff, Professor, University of Pittsburgh School of Law, Pittsburgh, Pennsylvania; Charles R. English, private practitioner,

English & Gold, Santa Monica, California; William H. Jeffress, Jr., private practitioner, Miller, Cassidy, Larocca & Lewin, Washington, D.C.; Michael Th. Johnson, Merrimack County Attorney, Concord, New Hampshire; Henry H. Kennedy, Jr., Judge, Superior Court, Washington, D.C.; Irma S. Raker, Judge, Maryland Court of Appeals, Rockville, Maryland; Norman K. Maleng, King County Prosecutor, Seattle, Washington; Norval Morris, Professor, University of Chicago Law School, Chicago, Illinois; and Jo-Ann Wallace, Director, Public Defender Service for the District of Columbia, Washington, D.C. The following persons also served as liaisons to the Committee: M. L. Ebert, Jr. from the National Association of Attorneys General; Harold Entz from the ABA Judicial Division; Addie Hailstorks from the National Legal Aid and Defender Association; Mary Frances Harkenrider from the U.S. Department of Justice; and Robert M. A. Johnson from the National District Attorneys Association. Judith White McBride served as Project Director until May 1997.

Dedication

The Task Force on Technology and Law Enforcement dedicates its work on the *Electronic Surveillance Standards* to Eric M. Noonan who diligently, intelligently, and with good humor and common sense served as Task Force Liaison from the National Association of Attorneys General until his untimely death on April 24, 1999.

Task Force:
Technology and Law Enforcement

Sheldon Krantz, Chairperson
Private practitioner, Piper & Marbury, Washington, D.C.

Walter Bruce Brownridge
General Counsel, Cleveland Police Department,
Cleveland, Ohio

James G. Carr
Judge, United States District Court, Toledo, Ohio

Scott Charney
Chief, Computer Crime and Intellectual Property Section,
Criminal Division, U.S. Department of Justice,
Washington, D.C.

John S. Farrell
Chief, Prince George's County Police Department,
Palmer Park, Maryland

Andrew Good
Private practitioner, Silverglate & Good, Boston, Massachusetts

Samuel A. Guiberson
Private practitioner, Guiberson Law Office, Houston, Texas

Richard Huffman
Justice, Fourth District Court of Appeals, San Diego, California

Wayne R. LaFave
Professor, University of Illinois College of Law, Champaign, Illinois

Gail Thackeray
Special Counsel, Technology Crimes, Office of the Attorney General,
Phoenix, Arizona

Christopher Slobogin, Reporter
Stephen C. O'Connell Professor of Law, University of Florida
Fredric G. Levin College of Law, Gainesville, Florida

Liaisons to the Technology and Law Enforcement Task Force

Laura Champlain
National Security Agency
Ronald Goldstock
ABA Criminal Justice Section Council
Mary Frances Harkenrider
U.S. Department of Justice
Albert J. Krieger
National Association of Criminal Defense Lawyers
Eric M. Noonan
National Association of Attorneys General
Lynn M. Pierce
Federal Bureau of Investigation
Ronald L. Plesser
ABA Individual Rights and Responsibilities Section
Terrence Sheridan
Major City Chiefs
Jo-Ann Wallace
National Legal Aid and Defender Association
Brad Wiegmann
U.S. Department of Defense
Kevin L. Wright
National District Attorneys Association

Technology and Law Enforcement Task Force Associates

Gina DiGiuseppe
U.S. Department of Justice, Washington, D.C.
Mark Eckenwiler
U.S. Department of Justice, Washington, D.C.
Mark G. Spurrier
Baltimore County Police Department, Baltimore, Maryland
Janet D. Webb
U.S. Department of Justice, Washington, D.C.
Julie Wuslich
U.S. Department of Justice, Washington, D.C.

Staff to the Technology and Law Enforcement Task Force

Susan W. Hillenbrand
Project Director
Aaron Sheppard
Project Assistant

During the preparation of the Technologically-Assisted Physical Surveillance Standards, Marc Rotenberg, Director, Electronic Privacy Information Center, Washington, D.C., also served on the Task Force. The following persons also served as liaisons to the Task Force: James M. Catterson from the National District Attorneys Association; Harold Entz from the ABA Judicial Division; Samuel A. Guiberson from the ABA Criminal Justice Section Science and Technology Committee; William J. Johnson from the National Association of Police Organizations; Lionel P. Kennedy from the National Security Agency; Emil P. Moschella from the Federal Bureau of Investigation; R. Hackney Wiegmann from the U.S. Department of Defense; and Stuart Wirtz from the Federal Bureau of Investigation. The following persons also served as associates to the Task Force: Hilary Conner, Deputy District Attorney, Philadelphia, Pennsylvania; Phil Reitinger, Trial Attorney,

Computer Crime Unit, U.S. Department of Justice, Washington, D.C.; and Daniel Weitzner, Deputy Director, Center for Democracy and Technology, Washington, D.C.

Contents—Electronic Surveillance Standards

Section B: Technologically-Assisted Physical Surveillance

INTRODUCTION

Background of the Standards

Three decades ago the American Bar Association promulgated its Standards Relating to Electronic Surveillance, which provide detailed guidelines for conducting electronic eavesdropping of communications.[1] Work on those standards helped define the debate over the limitations on wiretapping and bugging, and heavily influenced subsequent federal legislation on the subject.[2] The drafters of the Electronic Surveillance Standards also considered producing guidelines for the use of video surveillance and related surveillance techniques. Ultimately, however, they refrained from doing so. As they explained, "[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 [any] attempt to go beyond that experience now would be premature."[3] The drafters added, "[w]ith more knowledge, other action can be taken in the future."[4]

In 1995, the ABA's Criminal Justice Standards Committee decided that the time for such action had come. In that year, it appointed a Task Force on Technology and Law Enforcement, charging it not only with suggesting revisions to the Second Edition Electronic Surveillance Standards but also with developing guidelines for use of other technological surveillance techniques. Comprised of prosecutors, criminal defense lawyers, law enforcement officials, judges, privacy experts, and academics, the Task Force endeavored to identify and assess the primary constitutional and policy issues that are raised when technology is used to solve and prevent crime. In carrying out this objective, the Task Force consulted scores of organizations, ranging from national law enforcement agencies and local police departments to technology experts and advocates for individual privacy.

---

1. ABA Standards for Criminal Justice Relating to Electronic Surveillance (1st ed. 1971).
2. *See* 18 U.S.C. §§ 2510-20 (1968).
3. Electronic Surveillance Standards, *supra* note 1, at 104.
4. *Id.*

The Standards Committee carefully examined the Task Force's recommendations in the course of arriving at the final version of the standards, which the Committee unanimously approved in March 1997. These standards were submitted for first reading to the Criminal Justice Section Council in November 1997 and were finally approved by the Council in March 1998, with one dissenting vote. On August 3, 1998, the ABA House of Delegates officially promulgated the standards, which will form a new section of the Third Edition Electronic Surveillance Standards. While this section is somewhat interrelated with the section on communications surveillance,[5] revision of which is not complete, these Technologically-Assisted Physical Surveillance Standards are sufficiently independent and of sufficient public import that the Standards Committee decided to issue them separately at this time. As the commentary explains, they combine a restatement of basic Fourth Amendment principles with aspirational goals that are intended to secure privacy in a world of increasingly sophisticated technology.

The Scope of the Standards

These standards deal with *physical surveillance* that is *technologically-assisted* and that is used for *law enforcement* purposes. *Physical surveillance* involves observation or detection of activities, conditions, locations, or objects. It is to be distinguished from communications surveillance, which entails interception of conversations and other communications and has already been addressed in the Electronic Surveillance Standards. It should also be distinguished from transactional surveillance, or the accessing of recorded transactions, a topic which may eventually be the focus of subsequent standards.

The term "*technologically-assisted physical surveillance*," as used in these standards, is meant to refer to physical surveillance using technology, in particular surveillance using any one of five different types of technology: "video surveillance"; "tracking devices"; "illumination devices"; "telescopic

5. *See*, in particular, Standard 2-9.3(a).

devices"; and "detection devices" (*i.e.*, devices capable of detecting concealed items). These categories reflect the basic types of surveillance activity that are prevalent enough to warrant concern. While the Standards Committee anticipates that new and increasingly sophisticated technologies will continue to emerge, most future technologies should fall into one of these five categories.

The capabilities of technological physical surveillance techniques may come as a surprise to those who have not followed developments in surveillance equipment. For example, video technology, although available for some time, has seen dramatic advances in the past three decades. With the advent of wide-angle and pinhole lenses, night vision equipment, and super-magnification capacity, video surveillance allows viewing of home interiors, workplaces, and public thoroughfares at all times of the day and night. Cameras can be placed in picture frames, briefcases, pens, suit lapels, and teddy bears, allowing covert observation in virtually any circumstances. They also can be used overtly and conspicuously, to surveil private establishments and public places. Furthermore, any surveillance by camera can be recorded, permitting a permanent record of activities within the camera's range.

Tracking devices also come in many forms. One of the simplest is the beeper, which emits a signal that can be traced electronically and can be placed in virtually any vehicle or item. Other tracking devices under development or already in use include radar that can monitor vehicles over the horizon; bistatic sensor devices that passively pick up various types of emissions (*e.g.*, from a cellular phone) or rely instead on an active sonar-like capacity; and tagging systems that use a projectile launcher to attach a beeper to a fleeing vehicle. Also of relevance here are efforts to construct "intelligent transportation systems," which involve fitting every vehicle in a given transportation network with radio units that transmit to a base station. While envisioned principally as a way of controlling traffic patterns, these systems will also provide a way of tracking individual vehicles, or of discovering where they were located at a previous point in time.

Unlike modern video surveillance and tracking systems, some types of telescopic and illumination devices—for example, binoculars and telescopes, flashlights and spotlights—have been available for more than century. Today, however, science has provided would-be viewers with significantly

greater capabilities to overcome obstacles created by distance and darkness. Compact night-vision equipment using infrared technology allows covert observation of any night-time activity, while map-making and satellite cameras are able to focus on objects a few feet across from thousands of feet in the air. Illumination and telescopic capacity can also be combined in one instrument.

Finally, detection systems have been developed that include a wide range of devices using x-rays, heat radiation sensors, holographic radar scanners, and other technologies. Simple metal detectors will soon be augmented by devices that can be held in the hand and discern shapes and sizes of items underneath a person's clothing and even behind walls; some of these devices may also reveal anatomical details. Other mechanisms have been developed for detecting hidden explosives and the "heat waste" that might signal use of klieg lights or furnaces connected with growth or manufacture of contraband.

These examples do not describe all possible types of technologically-assisted physical surveillance. They are provided simply to illustrate current and anticipated technology at the time these standards were developed. As noted, these standards were drafted under the assumption that the types and capabilities of technological devices that can be used to assist in criminal investigations will continue to emerge and expand.

A third defining characteristic of these standards is that they focus solely on *law enforcement* use of technologically-assisted physical surveillance. There is no doubt that purely private use of physical surveillance technology has also increased enormously in recent years. Indeed, corporate and personal use of video cameras, detection devices, and other physical surveillance technology is clearly outpacing physical surveillance by the government. It may well be that private use of these technologies should be significantly limited, and in some instances perhaps even prohibited, just as federal electronic surveillance law outlaws private use of communications interception equipment.[6] Many of the principles outlined in these standards for regulating the use of these technologies for law enforcement purposes may prove relevant to regulating private uses of these technologies. These

6. 18 U.S.C. § 2512.

standards, however, do not purport to provide guidelines for private surveillance.

Similarly, while these standards are meant to apply to most government uses of technologically-assisted physical surveillance, certain government agencies, such as the Secret Service, the National Security Agency, and some regulatory departments, may operate under special rules that would make application of these standards inappropriate. Other than these special circumstances, however, the standards reflect the view that government officials should not be subject to differing standards merely because they enforce different aspects of the law.[7] Thus, the term "law enforcement" as used in these standards is meant to be construed broadly to include not just the police, but other principal actors charged with using government authority to enforce the law, such as those agencies that run airports, prisons, and border operations.

Rationale for Issuing Standards at This Time

There is still much to learn about the effects of using technologically-assisted physical surveillance, and more sophisticated devices for carrying out such surveillance are continuing to emerge. But the Standards Committee concluded that any further delay in devising a regulatory scheme in this area would be ill-advised, for a number of reasons.

First, technologically-assisted physical surveillance has become routine practice in some law enforcement contexts. Some government agencies now commonly use video surveillance, tracking, illumination and magnification devices, and even detection devices. There is no doubt that such surveillance will continue to increase both in scope and in complexity. Some type of regulatory framework, even one that will require revision in the future, is needed.

---

7. *Cf.* New Jersey v. T.L.O. 469 U.S. 325, 335 (1985) ("[b]ecause the individual's interest in privacy and personal security 'suffers whether the government's motivation is to investigate violations of criminal laws or breaches of other statutory or regulatory standards,' it would be 'anomalous to say that the individual and his private property are fully protected by the Fourth Amendment only when the individual is suspected of criminal behavior.' ") (quoting Camara v. Municipal Court, 387 U.S. 523 (1967)).

Such a framework has not been forthcoming from the courts, which suggests a second reason for issuing these standards now: traditional legal doctrine does not necessarily answer many of the novel questions raised by the use of technologically-assisted physical surveillance. The constitutional provision most relevant to regulation of physical surveillance is, of course, the Fourth Amendment, which bans unreasonable searches and seizures and requires that warrants authorizing searches and seizures be based on probable cause. As currently interpreted by the courts, this constitutional guarantee does not apply to some types of surveillance techniques that nonetheless ought to be subject to some controls. For example, given its public nature, use of video cameras to scan the streets does not trigger the warrant or probable cause protections of the Fourth Amendment, yet most would agree that such surveillance should be subject to some sort of regulation. Equally important issues concerning accountability, such as whether the public ought to be apprised of how often surveillance technology is used, have traditionally fallen outside the ambit of the Fourth Amendment as construed by the courts.

Further, when the courts *have* tried to regulate technologically-assisted physical surveillance by the police, their efforts have not resulted in a consistent body of case law. The Supreme Court alone has proffered several different analytical approaches to regulation of physical surveillance.[8] In the lower courts, there is an even greater disparity in holdings. Some courts have concluded that thermal imaging of heat waves from a building requires a warrant,[9] while others have declared that this activity does not even implicate the Fourth Amendment.[10] Similarly, some courts have held that use of binoculars to look in the home is a search,[11] while others have said it is not.[12] Other examples of such diametrically opposed results are cited in the

---

8. *See* commentary relating to Standard 2-9.1(c).

9. United States v. Cusumano, 67 F.2d 3d 1497 (10th Cir. 1995), vacated by 83 F.3d 1247 (10th Cir. 1996); United States v. Field, 85 F.Supp. 1518 (W.D. Wis 1994).

10. United States v. Kyllo, 1996 WL 125594 (D. Or. 1996); United States v. Penny-Feeny, 773 F.Supp. 220 (D. Haw. 1991).

11. State v. Carter, 790 P.2d 1152 (Or.Ct.App. 1990); People v. Oynes, 920 P.2d 880 (Co.Ct.App. 1996).

12. *See, e.g.*, People v. Arno, 90 Cal.App.3d 505, 153 Cal.Rptr. 624 (1979).

commentary to these standards, which aim to enhance debate about these issues if not resolve them.

A final reason for issuing these standards now is to prompt non-judicial law-making in the area. Many of the questions left unaddressed or addressed inconsistently by the courts could be handled more satisfactorily by general standards issued by other law-making bodies, such as legislatures or law enforcement agencies. To date, these entities have yet to take up the challenge. In contrast to electronic surveillance of communications, technologically-assisted physical surveillance has never been the subject of comprehensive legislative oversight. Neither the existing ABA Standards on Electronic Surveillance nor Title III and its various successors at the federal level regulate technological enhancement of this type of investigation. State and local lawmaking bodies have also largely avoided the issue, and police departments generally lack rules on the subject.

At bottom, law enforcement agencies, judges, and others who must evaluate the propriety of using physical surveillance technology need more guidance than they now have, not simply in terms of specific rules but also with respect to the competing values to be weighed in making decisions about how and when to use these technologies in law enforcement. The Standards Committee, with the help of its Task Force, was able to draw on a wide body of knowledge and to assess the needs of law enforcement as well as the concerns of private citizens. The end result is a set of standards that incorporate both general provisions and detailed rules governing use of physical surveillance techniques. The Committee hopes that these standards will encourage the development—both by legislatures and administrative bodies—of even more specific written rules governing technologically-assisted physical surveillance.

An Overview of the Standards

Several fundamental aspects of the standards, all concerning their relationship to Fourth Amendment law, should be mentioned at the outset. These standards seek neither to expand nor contract those situations which require a warrant or a particular level of cause under the Fourth Amendment, nor are they intended to add to or detract from the constitutionally mandated

remedies for violations of that Amendment. At the same time, the standards recognize that there are areas in which Fourth Amendment principles alone may not provide adequate protection for the privacy and related interests that are implicated by the use of new technologies for criminal investigations. In these areas, they recognize that it may be desirable to enact, by legislative or administrative rule, protections that go beyond those recognized in current Fourth Amendment case law. No position is taken as to what remedies, if any, ought to apply to violations of such voluntarily-adopted measures. However, consistent with the ABA's Urban Police Function Standards,[13] the standards strongly encourage law enforcement organizations to develop more detailed rules reflecting these principles.

More specifically, the Technologically-Assisted Physical Surveillance Standards consist of six standards. The first standard sets out general principles. The second contains definitions. The final four standards govern specific surveillance techniques: video surveillance, tracking devices, illumination and telescopic devices (treated together), and detection devices.

Standard 2-9.1, the general principles standard, attempts to accomplish several goals. First, it lays the substantive groundwork for the specific standards that follow. It also sets forth general principles concerning execution of surveillance, the role to be played by different governmental entities in regulating surveillance, and the means by which accountability can be established. Finally, this initial standard is intended to provide guidance on issues not answered by the specific standards (such as whether, for example, a particular device, such as an ordinary flashlight, constitutes the type of technology that should be subject to regulation), as well as on issues that may arise in the future with respect to new technologies not encompassed within the specific standards.

The first three sections of Standard 2-9.1, (a), (b) and (c), lay out the competing governmental and individual interests that must be considered in determining the type of showing, if any, the government should be required to make before it may conduct such surveillance. No hierarchical significance should be attributed to the fact that this standard explains the need for technology, in paragraph (a), before it describes the need for

13. *See* commentary to ABA Standards for Criminal Justice Relating to the Urban Police Function 116-44 (1st ed. 1973).

regulating that technology, in paragraph (b). These needs are equally important. As a logical matter, however, regulation of technology would not be necessary if the technology itself were not needed.

The next section of the general principles, found in Standard 2-9.1, (d), provides guidelines for executing surveillance that has met the threshold showing, including rules governing the scope of the surveillance, notice requirements, and maintenance of records. Section (e) emphasizes that parties other than courts (*e.g.*, legislatures, elected public officials, law enforcement agencies, and the public) may have important roles to play in formulating policies on the use of new technology, and identifies factors that might be considered in determining the allocation and scope of those roles. Section (f) addresses accountability, which is especially important in light of the covert nature of much technologically-assisted physical surveillance. Section (g) stresses the importance of police rule-making, encouragement of which is a primary reason for promulgating these standards, as the introduction noted. Finally, section (h) affirms that the standards are not meant to create new enforceable rights, but rather are designed to guide police and other agencies in developing rules.

Standard 2-9.2 provides definitions for the four remaining standards, 2-9.3 through 2-9.6. As noted, these final four standards deal with use of video surveillance, tracking devices, illumination and magnification devices, and detection devices, in that order. Applying the factors in section (c) of the general principles, they describe the showing required for various uses of these technologies. In general, these four standards track Fourth Amendment law in requiring probable cause for surveillance of areas associated with a reasonable expectation of privacy (and a warrant in non-exigent situations), except in a few well-defined situations related to unusual hazard, where a showing either of reasonable suspicion or a compelling state interest suffices. When surveillance is of a nonprivate area or activity, the standards generally require that use of the surveillance be reasonably likely to achieve a legitimate law enforcement objective, a term defined in more detail in Standard 2-9.2(d). In some non-exigent settings they also require that a supervisory officer make this determination.

Not every investigative technological innovation can be fully anticipated in drafting standards. Nonetheless, the general principles set out in these standards and the application of those principles in the specific standards

should provide the basis for making the trade-offs between public safety and individual liberty that the advent of such future technology necessitates.

SECTION B.
TECHNOLOGICALLY-ASSISTED PHYSICAL SURVEILLANCE

Standard 2-9.1 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 citizens and officers, 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) 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.

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

(v) Notice of the surveillance should be given when appropriate.

(A) Pre-surveillance notice should be given by the appropriate authority when deterrence is the primary objective of the surveillance (as with some types of checkpoints) or when those potentially subject to the surveillance should be given the option of avoiding it.

(B) When a court order has authorized the surveillance, post-surveillance notice should be given by the appropriate

authority to those listed in the order, but can be delayed for good cause shown. Post-surveillance notice to the principal target(s) of the surveillance may also be appropriate for other surveillance requiring probable cause.

(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, the defense bar, 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 making this assessment depends on such factors as the:

(i) legal basis for the rule;

(ii) invasiveness of the surveillance;

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

(iv) value of sharing decisionmaking; and

(v) 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 exists;

(ii) the exclusionary sanction when, and only when, it is mandated by federal or state constitutions or legislation;

(iii) internal regulations promulgated pursuant to Standard 2-9.1(g);

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

(v) maintaining and making available to the public general information about the type or types of surveillance being used and

the frequency of their use. Sensitive law enforcement information need not be disclosed.

(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 2-9.3 through 2-9.6;

(ii) the rules developed by other agencies pursuant to Standard 2-9.1(e); and

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

(h) *Non-binding effect of standards.* Nothing in these standards is intended to create rights, privileges, or benefits not otherwise recognized by law. Rather, they are meant to ensure that surveillance decisions are based on all relevant considerations and information.

Standard 2-9.2 Definitions

The following definitions apply to Standards 2-9.3 through 2-9.6.

(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 *contraband-specific* if it can only reveal the presence of an object that 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, 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 area where it occurs or exists and other relevant considerations 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 2-9.3. 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 2-1.1 et seq. of this Chapter], as modified for video surveillance.*

(b) Overt video surveillance for a protracted period not governed by Standard 2-9.3(a) is permissible when:

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

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

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

(ii) in cases where deterrence rather than investigation is the primary objective, 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 2-9.3(a) or (b) is permissible when a supervisory law enforcement official, or the surveilling officer when there are exigent circumstances, concludes that the surveillance:

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

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

Standard 2-9.4 Tracking Devices

(a) Installation pursuant to paragraph (b)(i) and monitoring pursuant to paragraph (c)(i) shall be permitted only on written authorization by a judicial officer, except when obtaining the required

---

* This provision is subject to change, depending upon the Third Edition recommendations on communications surveillance.

court order is not feasible due to exigent circumstances, in which case it shall be obtained 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.

(b) 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.

(c) 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 sufficient basis under applicable constitutional principles to believe that such monitoring will reveal evidence of crime, provided that, if one or more of the subjects of the monitoring consents to have the tracking device accompany their person, 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.

Standard 2-9.5 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 2-9.5(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 2-9.6 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 conditions creating a lesser expectation of privacy associated with the private place;

(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;

(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 2-9.6(a) is permissible if it does not involve search of a place of residence or of a person 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 2-9.6(a)(iii), even absent any individualized suspicion of danger that otherwise would be required.

(d) Law enforcement agencies using detection devices shall 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.

STANDARDS WITH COMMENTARY*

SECTION B.
TECHNOLOGICALLY-ASSISTED PHYSICAL SURVEILLANCE

Standard 2-9.1 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 citizens and officers, the apprehension and prosecution of criminals, and the protection of the innocent.

Commentary to Standard 2-9.1(a)

Law enforcement has relied on technologically-assisted physical surveillance, broadly defined, for some time. In the last century, lanterns and telescopes provided simple but effective means of enhancing police investigation. The 1920's saw the advent of primitive tracking devices as a police surveillance tool. By the middle of this century police began using video cameras and electronic beepers for investigative purposes. It has only been since the 1970's, however, that truly sophisticated devices, many of them developed initially for military purposes, have found their way into the law enforcement arsenal.

This standard acknowledges the "need for surveillance" by recognizing that technologically-assisted physical surveillance—whether using old or new technology—benefits law enforcement agencies in several ways. First, it

---

* In the text below, the commentary follows each full standard, except with respect to the General Principles standard. Because of the length of that standard, commentary follows each subsection.

facilitates the "detection, investigation, prevention, and deterrence of crime," as well as the "apprehension and prosecution of criminals." For example, covert video surveillance allows police to observe activities they would not be able to see in person,[1] and permits corroboration of those activities they can observe. Tracking devices have been used to follow suspects, both across jurisdictional boundaries and for lengthy periods, to determine their contacts and destinations without incurring the enormous resources and the risk of discovery that visual tracking would have entailed.[2] Similarly, because they have sophisticated telescopic and illumination devices, police need not worry about giving themselves away when trying to observe activity that requires a close look or is occurring in a dark place.[3] And detection devices permit police to discover weapons and contraband which would otherwise go undetected without a full search of people, luggage, or houses.[4]

Technologically-assisted physical surveillance can also improve law enforcement's efforts in the deterrence of crime. Conspicuously mounted cameras on street corners may provide strong disincentives to potential criminals. Detection devices used in airports, courthouses, and other public buildings prevent the introduction of weapons and other contraband. Law enforcement relies on these devices to deter not only because they are effective at accomplishing that aim, but because they are often cheaper, more efficient, and less offensive to the general population than deterrence techniques using officers.

Finally, technologically-assisted physical surveillance can also protect "the safety of citizens and officers." Telescopic, illumination, and detection devices can be used to ascertain, prior to entry, the presence in a residence of occupants or arms. Detection devices make possible "electronic frisks"

---

1. In one case, for instance, even aural surveillance was fruitless because the suspects, possible terrorists, spoke in code or worked in silence; video cameras provided incriminating evidence of bomb-making. *See* United States v. Torres, 751 F.2d 875 (7th Cir. 1984).

2. *See, e.g.*, United States v. Knotts, 460 U.S. 276 (1983); United States v. Surrell, 35 F.3d 573 (9th Cir. Cal. 1994); United States v. Juda, 797 F.Supp 774 (Cal. 1992); State v. Campbell, 306 Or. 157 (Or. 1988).

3. *See, e.g.*, State v. Wacker, 856 P.2d 1029 (Or. 1993) (surveillance of a parked car using night vision system).

4. *Cf.* United States v. Lopez, 328 F.Supp. 1077 (E.D.N.Y. 1971) (use of magnetometer to electronically frisk airplane passengers).

of a suspect, car, or container from a distance. Here again, these devices may prove not only more effective but less costly and less intrusive than traditional means of protecting officers and the public.

Standard 2-9.1 General Principles

(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.

Commentary to Standard 2-9.1(b)

As discussion of Standard 2-9.1(a) illustrates, technologically-assisted physical surveillance is a potent law enforcement tool. At the same time, it has the potential to undermine a number of values considered important in our society, thus prompting this standard's focus on the "need for regulation."

The most obvious value implicated by physical surveillance is individual "privacy." As used in these standards, this concept includes those interests the Supreme Court has said define the Fourth Amendment threshold under *Katz v. United States*.[5] However, the concept is also meant to encompass more than the "reasonable expectation of privacy" the Supreme Court has recognized in connection with the Fourth Amendment. In a number of related contexts, such as those having to do with government attempts to obtain financial accounts,[6] phone records,[7] and other types of personal

5. 389 U.S. 347 (1967).

6. *See* Right to Financial Privacy Act, 12 U.S.C. §§ 3401 (1978) (permitting customers the opportunity to challenge federal subpoenas for financial records prior to their execution, unless such notice would "seriously jeopardize the investigation").

7. *See* Electronic Communication Privacy Act, 18 U.S.C. § 3121 (1987) (requiring prosecutors to obtain court approval before obtaining phone records)

information,[8] society has indicated its willingness to recognize privacy interests not protected by the Fourth Amendment. The word "privacy" in this standard is meant to reflect this more expansive understanding of privacy.

Standard 2-9.1(b) reinforces this more expansive approach by emphasizing that technologically-assisted physical surveillance can implicate other values as well, including "freedom of association, speech, and travel," and, more generally, the "openness of society." The latter concept includes the enjoyment of public anonymity—a general expectation that absent suspicious conduct, citizens will not be subjected to intensive official scrutiny.

The threat that technology poses to these various interests is, in part, the same type of threat posed by traditional law enforcement investigative techniques. But the economies of technology pose an additional challenge to individual freedom. When surveillance can be carried out by gadgets rather than people, and when the gadgets are mass produced at increasingly lower costs, then economics may no longer serve as a sufficient restraint. The ultimate threat of unregulated modern technology could be a stifling police presence which affects the innocent and guilty alike. Thus, Standard 2-9.1(b) concludes that law enforcement use of technologically-assisted physical surveillance "may need to be regulated."

Standard 2-9.1 General Principles

(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:

---

8. *See* Britt v. Naval Investigative Serv., 886 F.2d 544 (3d Cir. 1989) (holding that the Privacy Act, 5 U.S.C. § 552a (1994), may bar disclosure of information obtained by the Naval Investigative Service); Driver's Privacy Protection Act, 18 U.S.C. § 2721 (preventing use for prosecutive purposes of personal information in state motor vehicle records).

(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.

Commentary to Standard 2-9.1(c)

Standard 2-9.1(c) provides more specific guidance than the preceding two standards as to when "technologically-assisted physical surveillance should be regulated and, if so, to what extent." The general notion expressed in this standard is that there should be a balance between the government's and individual's interests defined in paragraphs (a) and (b) of Standard 2-9.1. In

some cases, surveillance will visit such a slight intrusion upon privacy and other values that no regulation may be necessary. For instance, briefly shining a flashlight on the outside of a house or scanning a parade as it passes through a public area using binoculars are not acts which diminish our sense of privacy or freedom. Nor is such a threat generally posed by serendipitous, as opposed to planned, police reliance on technology, as when a streetlamp happens to enable officers to observe nighttime activity. At the other end of the spectrum, on some occasions the intrusion may be so great that the government must demonstrate good reason at the probable cause level to carry out the surveillance, as for example with surveillance of locations inside the home.

The provisions of Standard 2-9.1(c) set out the factors that should inform this balancing of interests. They do not ascribe particular weights to any of the factors listed. However, the standards governing specific surveillance techniques found in Standards 2-9.3 through 2-9.6, which apply these factors, attempt to balance these values for each specific category of devices they address.

(i) Law enforcement interests. A fundamental consideration with respect to regulation of surveillance is the "law enforcement interests implicated by the surveillance." As defined in Standard 2-9.1(a), these interests consist of detection, investigation, prevention or deterrence of crime, protection of officers and citizens from harm, the apprehension or prosecution of criminals, and proving the innocence of others. This standard describes three ways these interests are relevant to the determination of whether, and to what extent, particular surveillance should take place.

Standard 2-9.1(c)(i)(A) indicates that "the nature of the law enforcement objective or objectives sought to be achieved" must be considered in this determination. Certain techniques may be reasonable only with respect to a particular law enforcement interest. For example, certain techniques (*e.g.*, at airport checkpoints) may be easier to justify for security purposes than for investigatory purposes. Similarly, certain measures (*e.g.*, an electronic "frisk" of a person on the street based on reasonable suspicion) may be permissible for protective purposes but not for detection or deterrence reasons.

The government's purpose in conducting the surveillance is also important in deciding what burden law enforcement must bear to justify a particular

procedure. The two traditional levels of justification under Fourth Amendment law are probable cause and reasonable suspicion, with the latter representing the lower level of certainty. The Supreme Court has consistently held that if the police engage in a "search," as that word is used in the Fourth Amendment, then probable cause is required when the police objective is to obtain evidence of crime.[9] On the other hand, some police searches conducted with the objective of protecting the police (*e.g.*, a frisk) are justifiable as long as a reasonable suspicion of danger exists.[10] Still other types of specialized enforcement activities that are primarily preventive in aim (often collectively referred to as administrative inspections or regulatory searches) are justified simply on the ground they are "reasonable," which usually is satisfied with either a lesser showing of individualized suspicion or a standardized routine that minimizes the risk of arbitrariness.[11]

Standard 2-9.1(c)(i)(B) lists as a second consideration "the extent to which the surveillance will achieve the law enforcement objective or objectives." A procedure which is not effective at what it purports to do should not be approved, no matter how significant the purpose it is designed to achieved. At the same time, certain procedures, such as the regulatory inspections just mentioned, may be thought permissible because other procedures, requiring more individualized justification, cannot achieve the government's legitimate objectives.[12]

---

9. *See, e.g.*, Arizona v. Hicks, 480 U.S. 321 (1987); Ybarra v. Illinois, 444 U.S. 85 (1979).

10. *See* Terry v. Ohio, 392 U.S. 1 (1968) (stop and frisk); Maryland v. Buie, 494 U.S. 325 (1990) (searches for confederates incident to an arrest).

11. *See* Camara v. Municipal Court, 387 U.S. 523 (1967) (authorizing residential health and safety inspections based on needs of area rather than condition of individual house); South Dakota v. Opperman, 428 U.S. 364 (1976) (inventory search pursuant to regulation permissible). *Cf.* Michigan State Police v. Sitz, 496 U.S. 444 (1990) (suspicionless stops at roadblocks to detect drunk drivers pursuant to state guidelines permissible).

12. *Cf.* Camara v. Municipal Court, 387 U.S. 523, 537 (1967) (holding that non-individualized probable cause with respect to health and safety violations justifies residential inspections, in part because a requirement of individualized probable cause would defeat the government's purpose); Skinner v. Railway Labor Executives' Ass., 489 U.S. 602, 631 (1989) ("A requirement of particularized suspicion of drug or alcohol use would seriously impede an employer's ability to obtain . . . information [about the cause of accidents], despite its obvious importance.").

A final consideration identified in Standard 2-9.1(c)(i)(C) as a legitimate law enforcement interest is the "nature and extent of the crime to be detected or deterred and of the harm to be protected against." This criterion is *not* intended to endorse a sliding-scale approach that changes the justification required for a particular form of intrusion based on the particular crime under investigation, an approach the Supreme Court has rejected on more than one occasion.[13] But consideration of the nature of the crime can legitimately enter into the articulation of rules governing surveillance techniques in at least three ways: (1) in the same fashion that has occurred in connection with wiretapping and electronic eavesdropping,[14] investigation of particularly private activities might be limited to specific crimes of a certain degree of seriousness; (2) less intrusive yet longer term surveillance, undertaken to detect or deter activities at a particular location (*e.g.*, covert video surveillance of public areas), might be permitted only when the extent of the crime problem at that place is serious; and (3) as the Supreme Court has observed,[15] the seriousness of criminal activity observed may justify one type of law enforcement action (*e.g.*, prevention based on reasonable suspicion) but not another (*e.g.*, detection based on reasonable suspicion).

(ii) Privacy considerations. Standard 2-9.1(c)(ii) makes clear that, in addition to gauging law enforcement interests, some measure of "the extent to which the surveillance techniques invades privacy" is important in establishing whether regulation is necessary and, if so, in determining the necessary degree of law enforcement justification (*e.g.*, probable cause

---

13. *See* Dunaway v. New York, 442 U.S. 200 (1979) (rejecting a "multifactor balancing test" based largely on "the gravity of the crime involved," which in this case would have given great weight to the fact that the police activity was directed at "solving a brutal crime which had remained unsolved for a period of almost five months"); Mincey v. Arizona, 437 U.S. 385, 98 S.Ct. 2408 (1978) (refusing to adopt a "murder scene" exception to the warrant requirement).

14. *See* 18 U.S.C.A. § 2516(1) (listing crimes which may be investigated using electronic surveillance).

15. *See* United States v. Hensley, 469 U.S. 221 (1985) (leaving open the possibility that stops on reasonable suspicion of *past*, as opposed to future, criminal activity might be impermissible if the crime is minor).

versus some lower level of suspicion).[16] This standard lists a variety of considerations which should inform the judgment about relative intrusion into privacy. While many of these considerations are also reflected in Supreme Court interpretations of the Fourth Amendment, it is the intent of these standards to adopt a concept of "privacy" that is not limited to and may be broader than the constitutional notion of a reasonable expectation of privacy.

(A) The nature of the place, activity, condition, or location surveilled. Standard 2-9.1(c)(ii)(A) begins the privacy analysis with consideration of the nature of the "place, activity, condition, or location." These terms are intended to be broad. "Places" range from houses to cars to containers. The term "location" is used to mean a particular area within a private place (*e.g.*, the space in front of a picture window). "Activity" is a self-explanatory term, but can be contrasted with "condition," which refers to objects in stasis or other circumstances that may be under surveillance. Consistent with case law on the subject, most of the following discussion focuses on privacy expectations associated with places.

Privacy expectations may be the greatest when the place surveilled is a person's private dwelling. Not surprisingly, given the Supreme Court's emphasis in *Katz* on expectations of privacy, the courts are most reluctant to allow unregulated enhanced surveillance when it focuses on the home, and traditionally a warrant is required to search such a place. This is true for technological as well as for traditional searches. For instance, the Supreme Court has held that use of a beeper to detect movement within a house is a search and requires some type of judicial authorization (although it is not clear whether probable cause or merely reasonable suspicion is required for such a warrant).[17]

On the other hand, when the surveillance is of an area outside the residence or similarly private building, the Fourth Amendment is often irrelevant. For instance, while use of a beeper to discover the contents of a house is a search, the Supreme Court has made clear that use of a beeper to detect movement

16. Relative intrusiveness is also relevant in determining which of various alternative techniques would constitute the lesser intrusion (an inquiry contemplated in Standard 2-9.1 (c)(iv)).

17. United States v. Karo, 468 U.S. 705 (1984).

on the public roads is not.[18] Also not a search, according to the Court, is use of an illumination device to inspect the interior of a car through the window,[19] the interior of a barn located on open fields,[20] or the outside of a boat.[21] Nor does use of telescopic equipment to surveil curtilage normally implicate the Fourth Amendment, at least when the curtilage is associated with a business.[22]

The nature of the "activity" or "condition" surveilled may also be a relevant consideration in the privacy analysis. In *California v. Ciraolo*,[23] the Court stated that *Katz'* rule protecting the privacy of conversations "does not translate readily into a rule of constitutional dimension that one who grows illicit drugs in his backyard is entitled to assume his unlawful conduct will not be observed by a passing aircraft."[24] Along the same lines, the Court has held that testing a substance strongly believed to be cocaine is not a search,[25] nor is a dog sniff of luggage which alerts the police only to the presence of contraband.[26] Observation of impersonal objects other than illicit substances may also be less subject to regulation. In *Dow Chemical v. United States*,[27] the Court noted that the aerial photographs taken in that case revealed only physical details of Dow's plant, not "identifiable human faces, secret documents," or other "intimate details."[28]

(B) The care taken to ensure privacy. Under Standard 2-9.1(c)(ii)(B), also relevant to the privacy analysis is the "care that has been taken to enhance the privacy" of a place, activity, condition, or location. Thus, in holding a flashlight inspection of a barn to be outside the Fourth Amendment's purview in *United States v. Dunn*,[29] the Supreme Court noted that the upper

---

18. United States v. Knotts, 460 U.S. 276 (1983).
19. Texas V. Brown, 460 U.S. 730 (1983).
20. United States v. Dunn, 480 U.S. 294 (1987).
21. Lee v. United States, 274 U.S. 559 (1927.
22. Dow Chemical Co. v. United States, 476 U.S. 227 (1986).
23. 476 U.S. 207 (1986).
24. 476 U.S. at 214.
25. United States v. Jacobsen, 466 U.S. 109 (1984).
26. United States v. Place, 462 U.S. 696 (1983).
27. 476 U.S. 227 (1986).
28. 476 U.S. at 239 n.5.
29. 480 U.S. 294 (1987).

portion of the "wall" through which police observed the interior consisted only of netting material.[30] In *Ciraolo*,[31] the fact that the defendant's fence was only ten feet high and thus would not have kept observers on a truck or a doubledecker bus from seeing his backyard helped justify the suspicionless aerial surveillance in that case, even though it was of residential curtilage.

In applying this standard, however, care must be taken to avoid ignoring the privacy interests of those who, for economic reasons, cannot take steps to protect their privacy. More importantly, placing too much reliance on the extent to which the target makes an effort to evade government surveillance would create the risk of encouraging a closed society, in which people routinely restrict their contact with the outside world. With the advent of the technologies at issue here, increasingly greater precautions (thicker walls, heavily curtained windows, avoidance of public exposure) would be necessary to render them ineffective. These standards are meant to reflect the view that a core privacy value should be recognized and respected which does not depend on the fortuities of the types of surveillance devices that may be invented, or the measures that may be created to thwart such devices.

(C) The lawfulness of the vantage point. Standard 2-9.1(c)(ii)(C) identifies the "lawfulness of the vantage point" as another consideration in the privacy analysis. Surveillance undertaken from a vantage point outside a private area is more likely to be unintrusive. In *Ciraolo*[32] and *Dow Chemical*,[33] the Supreme Court implied that had the government physically intruded upon the curtilage rather than flown over it, a search would have occurred, but since there was no intrusion, there was no search. Similarly, in *United States v. Place*,[34] the Court stated in dictum that a dog sniff of luggage is not a search in part because it does not intrude into the luggage.

---

30. *Dunn*, 480 U.S. at 298.

31. 476 U.S. 207 (1986).

32. 476 U.S. at 207 ("The observations . . . took place within public navigable airspace . . . in a physically nonintrusive manner. . . ").

33. 476 U.S. at 237 ("The narrow issue . . . concerns aerial observation of a 2,000-acre outdoor manufacturing facility without physical entry.").

34. 462 U.S. 696, 707 (1983) (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").

As to what constitutes a "lawful vantage point," clearly the street, a sidewalk, an apartment hallway, or public airspace would qualify. Private property can also be a "lawful" vantage point, despite the technical trespass involved. The Supreme Court has held that police can generally take up positions on any private property outside the curtilage without violating the Fourth Amendment.[35] And even curtilage might be a permissible vantage point if it is generally accessible to the public.[36] On the other hand, visual surveillance of the home from bushes on the property or a fenced-in backyard may be more than just a "technical" trespass.

(D) The availability and sophistication of the technology. Standard 2-9.1(c)(ii)(D) emphasizes the "availability and sophistication of the surveillance technology" as another relevant consideration. The overflight at issue in the Supreme Court's decision in *Dow Chemical* involved use of a mapmaking camera with a magnification capacity of 240. This fact did not give the Court pause, since the camera was purchasable on the "open market." However, the Court added, 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."[37] Further, 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 serious questions" than the camera-surveillance in *Dow Chemical*.[38]

Thus, the less "available" the particular surveillance equipment is and the greater its "sophistication," the more reason there may be to deem its use invasive. In contrast, widely-available or primitive surveillance techniques can be more easily anticipated and protected against, and thus less regulation may be appropriate.

---

35. United States v. Dunn, 480 U.S. 294 (1987) (viewing the interior of a barn from private open fields is not a search).

36. *See* Minnesota v. Carter, 119 S.Ct. 469, 480-81 (1998) (Breyer, J., concurring) (concluding that viewing an apartment kitchen from a ground floor window while standing in an area used by other apartment dwellers was not a search).

37. *Id.* at 238.

38. *Id.* at 239.

Yet here too caution must be exercised. The fact that equipment is sometimes used by the public or has not been prohibited for public use does not necessarily mean that use of the same equipment by government officials is always an insignificant invasion on privacy. Because many of the devices described above are already available to the public (*e.g.*, binoculars, telescopes, and mapmaking cameras), placing too much weight on this factor would significantly reduce privacy in the home and elsewhere. The Supreme Court recognized as much in *Florida v. Riley*,[39] where a majority indicated "that the reasonableness of Riley's expectation depends, in large measure, on the *frequency* of nonpolice helicopter flights at an altitude of 400 feet." [40] In other words, in *Riley* it was not enough to defeat the defendant's claim that a private person could buy a helicopter and fly at that level.

(E) The extent to which technology enhances the natural senses. Standard 2-9.1(c)(ii)(E) provides that the extent to which the surveillance technology "enhances the law enforcement officer's natural senses" is also relevant to the privacy analysis. For example, a satellite or a device that can penetrate visually through walls enhances one's senses to a much greater extent than most devices because it can "see" things that the police would never be able to see with the naked eye from an outside vantage point. Conversely, when an enhancement device is used simply to "confirm" something already seen by the naked eye (*e.g.*, use of binoculars to confirm an inadvertent sighting), its use is less likely to be seen as a search, even if the surveillance is of the home.[41] The idea that minimal enhancement of naked eye observation is not a search also finds some support in *Texas v. Brown*,[42] where the Supreme Court upheld the warrantless use of a flashlight to aid searching 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." [43]

---

39. 488 U.S. 445 (1989).

40. *Id.* at 705 (emphasis added) (Blackmun, J., dissenting) (noting that, given Justice O'Connor's concurrence and the four dissenting votes, a majority supported this position).

41. *See* United States v. Bassford, 601 F.Supp. 1324, 1335 (D.Me. 1985, *aff'd*, 812 F.2d 16 (1st Cir. 1987) (holding that use of binoculars is not a search when they give a "view of a readily visible marijuana plot previously observed with the naked eye").

42. 460 U.S. 730 (1983).

43. *Id.* at 740.

A related question, more difficult to analyze, is whether a search occurs when police use a surveillance device to see something that could have been viewed with the naked eye from a lawful vantage point but for fear that the surveillance would be discovered.[44] In such circumstances, the fact that a naked eye observer could not have viewed the activity without being discovered may be precisely why the target expects privacy. Whether such an expectation would be considered "reasonable," however, has yet to be resolved by the Supreme Court.

(F) Minimization of surveillance. Standard 2-9.1(c)(ii)(F) looks to the "extent to which the surveillance of subjects is minimized in time and space" as another privacy factor. Periods of surveillance that are "minimized in time" tend to be less intrusive than longer periods of surveillance. Following a vehicle by use of a tracking device for a hour is one thing, doing it for several days is quite another; using a nightscope to make a single, fast look into a building is one thing, but a fixed, long-term surveillance of the same character is another. Similarly, surveillance which reveals information or activity in a large physical "space" when surveillance of a smaller space would achieve the same government aim is suspect.

(G) Minimization of intrusion upon non-subjects. One reason that time and space dimensions are important to the privacy analysis is that they often bear upon the concern that government actions avoid unnecessary impact on innocent people. Standard 2-9.1(c)(ii)(G) emphasizes this concern by focusing on "the extent to which the surveillance of non-subjects is likewise minimized." The Supreme Court registered its hostility toward dragnet investigative techniques in *Davis v. Mississippi*,[45] where it reversed the conviction and death sentence of an African-American youth primarily because he had been one of 24 blacks taken into custody for fingerprinting, in a rape investigation in which the only lead was the victim's broad description of her assailant as a black youth. Along the same lines is Justice Brennan's dissent in *United States v. Jacobsen* cautioning against use of police dogs to "roam the streets at random, alerting the officers to people

---

44. *Cf.* 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).

45. 394 U.S. 721 (1969). *See also*, Hayes v. Florida, 470 U.S. 811 (1985).

carrying cocaine," or use of drug scanning devices "to scan all passersby" or "to identify all homes in which the drug was present."[46]

Conversely, in certain special circumstances the all-encompassing nature of the surveillance may actually be a critical factor in finding that the surveillance is proper. Pervasive group surveillance in a context in which everyone recognizes the danger of not doing so (*e.g.*, magnetometers in an airport) may not be considered intrusive, especially when individuals can avoid surveillance by walking away. In this type of situation, the pervasiveness of the search may make it *less* invasive, at least when everyone is subjected to it rather than allowing government to single out particular individuals without reason for suspicion (*see* Standard 2-9.1(d)(i)).

(H) Whether the surveillance is overt or covert. Under Standard 2-9.1(c)(ii)(H), the privacy analysis also takes into account "whether the surveillance is covert or overt." The Supreme Court has suggested that the intrusiveness of certain actions is reduced if those subjected to them are notified that they are occurring. For instance, in *United States v. Martinez-Fuerte*,[47] the Court upheld a roadblock established for the purpose of discovering illegal aliens in part because signs indicated where the checkpoint was, thus enabling motorists to avoid it. Surveillance that is overt in this manner may be less intrusive than covert surveillance, which, as emphasized later in this commentary, can pose special dangers to privacy precisely because its targets are unaware of it.

(iii) Infringement of other values. Standard 2-9.1(c)(iii) separately identifies the "extent to which the surveillance diminishes or enhances the exercise of First Amendment freedoms and related values" as another factor relevant to regulating the use of surveillance technology. These First Amendment interests represent values not encompassed by the privacy concept, as defined by the Supreme Court, but nonetheless deserving of some degree of protection.

As noted in connection with Standard 2-9.1(b), certain types of technologically-assisted physical surveillance may have a particularly

46. 466 U.S. at 138 (Brennan, J., dissenting).
47. 428 U.S. 543 (1976).

significant impact on the freedoms of speech, association and travel. For instance, publicly situated video cameras may chill legitimate but unpopular political activities. The same effect could be produced even by covert physical surveillance, if it is known or thought to be conducted under certain circumstances. This standard also requires that the extent to which surveillance may "enhance" First Amendment values be considered. In some circumstances, speech might not be able to take place without surveillance techniques that ensure security.

(iv) The least intrusive surveillance technique. A final consideration in weighing whether and to what extent technologically-assisted physical surveillance should be regulated is the "extent to which the surveillance technique is less intrusive than other available effective and efficient alternatives." Standard 2-9.1(c)(iv) recognizes that, even if surveillance can be justified under the foregoing analysis, the use of that technology may be ill-advised if less intrusive means are available and equally efficacious. While the Supreme Court has generally eschewed the so-called "least intrusive alternative" limitation in developing Fourth Amendment jurisprudence,[48] it has done so primarily because of concerns about judicial over-involvement in regulation of police decisionmaking.[49] Consistent with the Court's jurisprudence, this standard recognizes that the least restrictive means are appropriately considered by the police in devising their internal rules (a process otherwise encouraged by these standards, *see* Standard 2-9.1(g)).

---

48. 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.").

49. *See Lafayette*, 462 U.S. 640, at 647-48 ("it is not our function to write a manual on administering routine, neutral procedures of the station house . . . We are hardly in a position to second-guess police departments . . . ").

Standard 2-9.1 General Principles

(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) 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.

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

(v) Notice of the surveillance should be given when appropriate.

(A) Pre-surveillance notice should be given by the appropriate authority when deterrence is the primary objective of the surveillance (as with some types of checkpoints) or when those potentially subject to the surveillance should be given the option of avoiding it.

(B) When a court order has authorized the surveillance, post-surveillance notice should be given by the appropriate authority to those listed in the order, but can be delayed for good cause shown. Post-surveillance notice to the principal target(s) of the surveillance may also be appropriate for other surveillance requiring probable cause.

(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.

Commentary to Standard 2-9.1(d)

The previous provisions of Standard 2-9.1 focus on general principles governing when a intrusion via surveillance can be carried out. Standard 2-9.1(d) provides guidelines for the "implementation of the surveillance," which are meant to assure that justified surveillance is conducted properly. Its provisions apply to all of the specific surveillance applications addressed in Standards 2-9.3 through 2-9.6.

(i) The subjects of the surveillance should be fairly selected. Standard 2-9.1(d)(i) provides that the subjects of the surveillance "should not be selected in an arbitrary or discriminatory manner." Surveillance will often involve observation of groups of people or particular locations. In such situations, the government must be careful to avoid discriminatory practices. For example, selection of a checkpoint location because all who pass through that point are likely to be of a particular race would be intolerable. A technique that targeted only those who have little ability to muster political support for more evenhanded treatment would also raise serious concerns. These concerns, reflections of which can be found in Supreme Court case law,[50] exist even with procedures that do not visit any intrusion (*e.g.*, a device that can identify contraband and nothing else on a person, without any detention of that person).

This standard, then, mandates that by training, supervision and other appropriate means, law enforcement agencies should strive to ensure that all surveillance targets (whether a particular person or a particular group of persons, *e.g.*, all those passing a certain point or presenting themselves in a certain locale) are fairly selected. In addition, as to all surveillance activities which draw part of their justification from the fact that a large number of persons are being subjected to precisely the same form of limited intrusion, procedures should be in place to ensure that this equality in treatment occurs

---

50. This requirement can be fairly derived from the Supreme Court's decision in both Delaware v. Prouse, 440 U.S. 648 (1979) (finding unconstitutional vehicle stops that represented "unconstrained exercises of discretion") and Whren v. United States, 116 S.Ct. 1769, 1774 (1996) (stating that searches and seizures which result from intentional racial discrimination might provide relief under the Fourteenth Amendment).

and that particular individuals in the group are not unjustifiably singled out and scrutinized more intensively.

(ii) Limits on the scope of surveillance. Under Standard 2-9.1(d)(ii), the scope of surveillance should be "limited to its authorized objectives" and should "be terminated when those objectives are achieved." The first provision recognizes that, as required in connection with communications surveillance,[51] unnecessary visual intrusions must be minimized. The executing officers should be aware of the law enforcement objectives of the surveillance and should conduct the surveillance consistently with those objectives. Thus, if surveillance is not supposed to monitor private activities, it should not do so. For the same reason, surveillance should be conducted by the minimum number of officers necessary to carry it out.

The second provision is motivated by similar concerns. Virtually all forms of physical surveillance conducted by resort to sophisticated technology have the capacity for long-term use. For example, the electronic tracking of the movements of a person or vehicle might be conducted for hours or for days, as might a telescopic or illumination-aided surveillance at a fixed location. As described in connection with Standard 2-9.1(c)(ii)(F), normally the longer such surveillance is conducted, the greater the intrusion upon those who are the objects of such surveillance.

Thus, a meaningful regulatory scheme must include provisions regarding when surveillance procedures must be terminated. Termination of surveillance is obviously called for when the objective of the surveillance has been realized. More difficult is the question of when termination must occur absent such success, and the same answer may not be appropriate for all types of procedures. Some should have fixed time limits, at least absent an extension granted by the authorizing person or agency. In other instances, it may suffice that the surveilling officers are required to establish why they find the surveillance sufficiently promising to continue it.[52]

---

51. *See* 18 U.S.C. § 2518(4).

52. *Cf.* 18 U.S.C.A. § 2518(5) (requiring renewal warrants every 30 days for electronic surveillance).

(iii) The most restrictive rules should apply. Standard 2-9.1(d)(iii) deals with the regulatory quandary that arises when physical surveillance technology combines various functions. It provides that where a surveillance device makes use of "more than one regulated technology and the technologies are governed by differing rules, the more restrictive rules should apply." For instance, use of a satellite camera to surveil public areas could fall under provisions dealing with use of video technology (which in these standards require approval by at least a supervisory official) or provisions governing telescopic devices (which in these standards leave the surveillance decision up to the surveilling officer). This provision states that the more restrictive rule (*i.e.*, in this example, the video provisions) would apply.

(iv) Limitations on novel technology. Standard 2-9.1(d)(iv) addresses the issue of new technologies. It provides that the particular surveillance technique used "should be capable of doing what it purports to do" and should be "used solely for that purpose by officers trained in its use." New surveillance technologies are flooding the market. Law enforcement agencies must be aware that advertised capabilities are sometimes overblown. Ensuring that technological devices have been adequately tested or at least are capable of doing what they purport to do not only protects against unnecessary searches and arrests of innocent individuals, but also prevents dismissals of prosecutors' cases for insufficient evidence.[53] For the same reasons, sophisticated devices should only be used by those trained in their application.

(v) Notice of the surveillance. Standard 2-9.1(d)(v) specifies that "notice of the surveillance should be given when appropriate." The standard goes on to deal with both pre-surveillance notice and post-surveillance notice.

For obvious reasons, Standard 2-9.1(d)(v)(i) provides that pre-surveillance notice "should be given when deterrence is the primary objective of the

---

53. *Cf.* Fla. Stat. § 319.1905(1) (requiring testing of automobile speed measuring devices at least every six months, according to procedures prescribed by the department); Fla. Stat. § 319.1932 (1)(f) (requiring state Department of Law Enforcement to develop rules that "specify precisely the tests or tests to be used" for measuring blood alcohol and requiring that an approved method of administration be followed in all cases).

surveillance." The standard also provides that pre-surveillance notice should be given "when those potentially subject to the surveillance should be given the option of avoiding it." As the Supreme Court has recognized,[54] in some situations such notice might render an otherwise unreasonable police action reasonable by affording people the option of avoiding it. This could occur fairly often in connection with certain types of surveillance (*e.g.*, video surveillance of a street; use of detection device checkpoints), where people would rather not be subjected to the feeling of being observed or the inconvenience of a brief stop.

Standard 2-9.1(d)(v)(ii) deals with *post*-surveillance notice. It provides that when a court order has authorized the surveillance, such notice should be given "to those listed in the order" except when the judge determines that delay is necessary for "good cause" (*e.g.*, to prevent compromising law enforcement objectives). It also provides that post-surveillance notice may be advisable after warrantless surveillance where "probable cause" was required. As with communications surveillance,[55] this notice need not disclose precisely what was observed or detected. But it should alert the target of the surveillance to the time, place and duration of the surveillance.

Such post-surveillance notice requirement may be justified on two grounds. First, because covert surveillance can reveal as much to the police as the traditional search and seizure, its targets are entitled to the same degree of notice (and the concomitant ability to seek any available redress) that those subjected to overt searches and seizures automatically receive. It is probably for this reason that the Supreme Court, in *Berger v. New York*,[56] strongly suggested that post-surveillance notice is constitutionally required in the communications surveillance context. Second, to the extent it prompts a target to bring the surveillance to the attention of the public, a post-

---

54. 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.").

55. *See* commentary to ABA Standards for Criminal Justice, Electronic Surveillance, Standard 2-5.14 (2d ed. 1978).

56. 388 U.S. 41, 70 (1967).

surveillance notice requirement can also provide a means of holding government accountable for its actions.

However, requiring post-surveillance notice for all covert surveillance would be unduly burdensome and perhaps impossible. While surveillance requiring individualized suspicion is likely to focus on only one individual, or at least on only a few individuals, surveillance which does not require probable cause might encompass scores of people, some of whom may be difficult to identify or locate subsequent to the surveillance. Because this type of surveillance is generally not as intrusive as the traditional search and seizure, specific notice should not be required in such circumstances. The general injunction, in Standard 2-9.1(f)(v) below, that the public be apprised of the breadth and frequency of technologically-assisted surveillance should provide sufficient information about these less intrusive actions for public accountability purposes.

(vi) Use of surveillance results. Standard 2-9.1(d)(vi) provides that disclosure and use by law enforcement officials of information obtained through technologically-assisted physical surveillance "should be permitted only for designated lawful purposes." This standard reflects the conclusion that even if obtained properly, the information derived from physical surveillance must be carefully controlled, for two reasons.

First, the propriety of a search or seizure depends in part upon what is done with the information obtained.[57] Even if the police have full probable cause to search a house, a decision to display all of its contents in the public square is unreasonable.[58] Second, the dissemination of information may itself be an invasion of privacy. Such dissemination may be permissible if it is consistent with the purpose of a duly authorized search. But if the information or evidence obtained is used for other purposes, as in the above example, a violation of privacy rights may occur.

---

57. Several Supreme Court cases suggest that Fourth Amendment standards differ depending upon whether the evidence obtained in a search and seizure will be used for criminal or regulatory purposes. *See* O'Connor v. Ortega, 480 U.S. 709, 729 n.* (1987); Skinner v. Railway Labor Executives' Association, 489 U.S. 602, 621 n.5 (1989).

58. *Cf.* Wilson v. Layne, 119 S.Ct. 1692 (1999) (finding unreasonable media presence during the search of a house).

By limiting disclosures to "designated" lawful purposes, this standard expresses a preference that such disclosures be prohibited unless affirmatively authorized by a statute, judicial decision, or agency rule. The reasons for this approach are threefold: (1) compared to a decision by a lower level official, legislative, judicial, or agency action is more likely to be based on consideration of all the complex state and individual interests involved;[59] (2) disclosures motivated by discriminatory or vindictive motives are less likely; and (3) review of any disclosure decision is facilitated.[60]

(vii) Retention of recordings. Standard 2-9.1(d)(vii) addresses the related issue of the need to place limitations on government retention of recordings of surveillance. Not only video surveillance but also the results of tracking operations and the images produced by detection devices can be preserved well after the surveillance ends, in theory indeterminately. This capability raises the specter of extensive libraries that retain information on vast numbers of individuals in perpetuity. This standard deals with this problem by providing that "protocols should be developed for the maintenance and disposition of surveillance records not required to be maintained by law." A more bright-line approach, analogous to the preferred approach with respect to disclosure described above, would be to destroy such records unless the law directs otherwise. Destruction would occur either after the records are used for their intended law enforcement purpose, or when that purpose is no longer likely to be achieved.[61] This standard does not endorse that approach, however, because records can often have unanticipated benefits, not just in terms of incriminating the culpable, but also as a method for absolving the innocent. Such records might even be useful in demonstrating abuses by police agencies or in refuting false claims of such abuse. Instead, therefore,

---

59. As the Court recognized in Michigan 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.

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

61. In Baltimore, for example, records of public video surveillance are destroyed after 96 hours unless the recording becomes relevant to a criminal incident identified within that time period. Baltimore Video Patrol Program, Departmental Regulations, p. 2 (1999).

the standard requires that agencies develop clear rules for maintaining (and destroying) records, limited of course by any laws that are passed.

Standard 2-9.1 General Principles

(e) ***Rule-making and decision-making entities.***

A variety of entities, including the courts, legislatures, executive officials, prosecutors, the defense bar, 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 making this assessment depends on such factors as the:

(i) legal basis for the rule;
(ii) invasiveness of the surveillance;
(iii) need for deference to expertise in law enforcement;
(iv) value of sharing decisionmaking; and
(v) number of people and size of the geographic area affected by the surveillance.

Commentary to Standard 2-9.1(e)

Most of the rules governing search and seizure have come from the courts in cases argued by prosecutors and defense attorneys, with legislatures and police agencies playing a very secondary role. In deciding whether a particular search technique conforms to those rules, courts and police in the field have played the predominant roles. Standard 2-9.1(e) recognizes that, at least in the surveillance context, other entities, including legislatures, supervisory officials and the public, can be involved both in rule-making and in decisionmaking.

This standard is also meant to provide guidance as to when these various entities are best relied upon in connection with rule- and decisionmaking. It seeks to do so by reference to five factors: (1) the "legal basis of the rule" (which might dictate that certain entities—such as courts when the Constitution is implicated—be involved); (2) the "invasiveness of the

surveillance" (with greater invasiveness suggesting that a judge, or some other person removed from the conduct of the surveillance, be consulted); (3) the "need for deference to expertise in law enforcement" (most likely to be dispositive in constructing detailed procedures governing use of particular technologies); (4) the "value of sharing decisionmaking" (particularly important when surveillance of large groups is involved); and (5) the "number of people and size of the geographic area affected by the surveillance" (with municipal, state and federal legislatures more likely to be involved as these factors grow). The discussion that follows is organized around what roles the various decisionmaking entities might play in light of these factors.

Courts as Rulemakers and Decisionmakers

Where the rule is of constitutional origin, the courts, aided by the arguments of prosecutors and defense attorneys, have traditionally played a significant role. Even when the federal constitution is not implicated, courts interpreting state constitutional law or the common law can and have been heavily involved in developing rules governing governmental invasion of privacy and related rules.[62] The judiciary has often functioned as the ultimate protector of privacy in this regard.

Because they depend upon the fortuity of a case or controversy and are often limited to their facts, however, court-devised rules may not be the best way of devising a comprehensive regulatory scheme. Furthermore, where the Constitution is silent, courts may have no authority to devise a rule. For instance, as noted, surveillance of public areas is not governed by the Fourth Amendment. Similarly, rules regarding disclosure or retention of records may not be governed by constitutional doctrine.

A separate question from the proper source of the rules to be applied is which entity or entities ought to decide whether a particular surveillance may

62. Eleven state constitutions protect privacy in provisions or clauses separate from their search and seizure provisions. JENNIFER FRIESEN, STATE CONSTITUTIONAL LAW §2.02[1]. State courts have been active in interpreting these provisions. *Id.* § 2.03. In other states, courts have recognized privacy as a penumbral right. *Id.* § 2.01[2]. Privacy rights have also been developed at common law. See PROSSER & KEETON ON TORTS, ch. 20 (Privacy).

take place under them. Again, if the surveillance is a Fourth Amendment search requiring probable cause and is not conducted in exigent circumstances, a judicial officer must generally make the determination. In other circumstances, however, no particular decisionmaker is mandated.

Legislatures as Rulemakers and Decisionmakers

Because it is not subject to the case and controversy limitation and can be based on a wider array of information than judicial opinions, legislation can assume a prominent rule-making role. Legislation can both strengthen controls concerning conduct covered by the Fourth Amendment (as with existing legislation on wiretapping and electronic eavesdropping[63]), and create controls over conduct not touched by the Fourth Amendment (as with existing legislation regarding bank records and pen registers[64]). It can be relatively detailed or, when the need is for greater flexibility and the expertise of enforcement agencies, might instead mandate rule-making on a certain subject and of a certain type by law enforcement agencies. While the examples given above involve federal legislation, state and local law-making bodies can also play a role in this regard. This may be especially true in connection with physical surveillance, in contrast to communications surveillance, where the interstate nature of the problem has led to a federal role approaching preemption of the field.[65]

Legislatures might also be involved in deciding whether particular surveillance should take place. When the contemplated surveillance is to be more or less permanent and encompass virtually the totality of the governed, as with video cameras in subways, the political process can provide meaningful limitations upon the surveillance activity. When the universe of those to be surveilled becomes smaller and takes on characteristics unlike those of the total population, on the other hand, reliance on the majoritarian political process may have limitations. In such situations, oversight by other

---

63. *Cf.* 18 U.S.C. § 2510 et. seq.

64. 18 U.S.C. § 3401 (1978) (bank records); 18 U.S.C. § 3121 (1986) (pen registers).

65. *Cf.* 18 U.S.C. § 2516(2) (providing that a state court judge may grant an eavesdropping order only if the entire application process is in conformity with federal law as well as applicable state statutes).

decisionmakers instead of or in addition to legislative bodies might be preferable.

The Public as Decisionmaker

The public may also have a significant role to play in determining the advisability of surveillance techniques. For example, if the police and/or city council are contemplating placing overt surveillance cameras in a particular residential area, the reaction of those residing there is relevant for two reasons: they are the intended beneficiaries of the crime deterrence effort, and they are the persons who will bear the brunt of the surveillance. Furthermore, public input which provides the police with information about the nature and extent of crime can be helpful to the development of rational decisions about where to establish surveillance activity and what kind of surveillance to undertake.

In surveying public opinion, however, special care must be taken to solicit the perspectives of those *most* affected by the surveillance. As with the legislative process, reliance on the views of groups that have only a tangential stake in either the crime problem being addressed or the area contemplated for surveillance may skew analysis of the likely efficacy and impact of the surveillance.

Administrative Agencies and Police as Rulemakers and Decisionmakers

As the ABA Standards on the Urban Police Function recognize, "administrative rule making by police agencies" about "investigative techniques, and enforcement methods" is crucial.[66] Such self-regulation is most obviously necessary when mandated by state or local legislative bodies. But it is also appropriate when no such mandate exists, because it forces police to think about local problems, takes advantage of their expertise on this issue, and ensures better compliance than when rules are imposed from the outside. Indeed, this mode of regulation is so important that a specific

66. ABA Criminal Justice Standard 1-4.3 (2d ed. 1979).

provision (*see* Standard 2-9.1(g) below) is included to emphasize its necessity.

Police also inevitably play a significant role in deciding whether particular surveillance should take place. In those situations in which the Constitution allows decisions about probable cause, reasonable suspicion, or reasonable necessity to be made by someone other than judges, the officer conducting the search often has that responsibility. However, to assure that the objectives set out in Standards 2-9.1(c) and (d) are met, ultimate control of technological surveillance may need to rest in the hands of some entity or individual other than a field officer, at least in the absence of exigent circumstances. Consistent with the administrative model of decisionmaking described above, a primary candidate for such a role is a police supervisor. Decisions regarding non-exigent surveillance on individualized suspicion would be reserved for supervisory officers. So would decisions regarding surveillance activities that find their justification in the frequency of criminality at a certain location. In the latter situation, supervisory involvement (perhaps even at a higher level than for individualized surveillance) is particularly important, as the grounds for surveillance relate to the *department's* collected data on crime patterns in the community.

Standard 2-9.1 General Principles

(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 exists;

(ii) the exclusionary sanction when, and only when, it is mandated by federal or state constitutions or legislation;

(iii) internal regulations promulgated pursuant to Standard 2-9.1(g);

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

(v) maintaining and making available to the public general information about the type or types of surveillance being used and the frequency of their use. Sensitive law enforcement information need not be disclosed.

Commentary to Standard 2-9.1(f)

Standard 2-9.1(f) addresses "accountability and control" over those who conduct surveillance. Rules establishing accountability are particularly important in connection with technologically-assisted physical surveillance because most forms of it share a troublesome characteristic: the objects of the surveillance are totally unaware it is happening. The typical search and seizure is either observed by its target or leaves recognizable traces of its occurrence, and thus facilitates challenges to official misconduct. Technologically-assisted physical surveillance, by contrast, may never become known to its subjects. Thus, it is imperative that a system of control and accountability exist regarding all surveillance activities involving significant intrusions into privacy or similar values.

The various components of such a system are listed in Standard 2-9.1(f). This standard recognizes that exclusion of evidence is appropriate when required by the case law, but relies primarily on administrative monitoring and sanctions, along with dissemination of information about surveillance practices to the public. Together, these various elements should provide sufficient assurance that government use of technologically-assisted physical surveillance, whether covert or overt, adheres to the rules regarding justification and implementation.

(i) Administrative rules ensuring information about surveillance. Standard 2-9.1(f)(i) calls upon police and enforcement agencies to adopt "administrative rules which ensure that the information necessary for such accountability exists." Especially when use of surveillance is not memorialized through a warrant and its accompanying paperwork, police agencies need to develop rules that ensure specific surveillance actions are monitored.

Such monitoring might take place in a number of ways. For instance, use of surveillance techniques could be routinely documented, either by the field officer or the supervisor; such documentation might be particularly advisable when officers use sophisticated physical surveillance technology. Alternatively, supervisors could periodically or randomly observe surveillance. Technology itself could also be enlisted in the effort to acquire information; video recordings provide a fairly good clue as to how video surveillance was conducted. In short, police agencies should experiment to find methods that provide "sufficient information to ensure accountability."

(ii) Exclusion. Standard 2-9.1(f)(ii) takes the position that accountability should be ensured through use of the "exclusionary sanction when, and only when, it is mandated by federal or state constitutions or legislation." Thus, these standards are not meant to expand or contract the current scope of the exclusionary rule. The standards incorporate existing Fourth Amendment case law on this issue and take no position with respect to legislatively or administratively created rules of exclusion.

As the law stands today, when police fail to abide by strictures established by the Fourth Amendment or state constitutions, exclusion from the prosecution's case-in-chief is the proper remedy (unless the police rely in good faith on a judicially issued warrant).[67] Exclusion may be appropriate in other situations as well.[68] It is important to remember, however, the Supreme Court's admonition in *United States v. Caceres*[69] about expanding the reach of the exclusionary remedy outside the constitutional context. To mandate exclusion for violation of an administrative regulation, the Court stated, "would take away from the Executive Department the primary responsibility for fashioning the appropriate remedy for the violation of its regulations" and, in any event, might well be counterproductive because it would discourage "the formulation of additional standards to govern prosecutorial and police procedures."[70]

---

67. Mapp v. Ohio, 367 U.S. 643 (1961); United States v. Leon, 468 U.S. 897 (1984).

68. *Cf.* 18 U.S.C.A. § 2518(10)(a) (requiring exclusion if statutory violations, not amounting to constitutional violations, occur).

69. 440 U.S. 741 (1979).

70. *Id.* at 755-59.

(iii) Internal sanctions. Standard 2-9.1(f)(iii) calls for the promulgation of "internal regulations" providing written guidance to law enforcement officers. It is essential that law enforcement agencies establish a meaningful complaint and discipline system that will afford the public assurance that misconduct by officers will be identified and dealt with. Indeed, even when exclusion or compensatory and punitive damages are available, the most effective way of motivating police conformance with rules may well be enforcement by the police agency itself. Such sanctions should be promulgated pursuant to Standard 2-9.1(g), as described below.

(iv) Periodic review. Standard 2-9.1(f)(iv) calls for "periodic review by law enforcement agencies of the scope and effectiveness of technologically-assisted physical surveillance." Here the focus is not review of any particular surveillance, which was the subject of the administrative rules called for by Standard 2-9.1(f)(i), but rather an assessment of how effective certain types of surveillance have been at achieving their objectives (*e.g.*, aerial telescopic surveillance undertaken for purposes of drug interdiction; detection device checkpoints to confiscate or deter possession of weapons; publicly-mounted cameras to deter crime). This review can take place in conjunction with the collection of information necessary to satisfy Standard 2-9.1(f)(v)'s requirement, discussed below, that information about technologically-assisted physical surveillance be disseminated to the public. Without such assessments, the tendency may be to leave ineffective surveillance regimes in place, either out of inertia or unsupported intuition that they are working, resulting in unnecessary compromises of privacy and freedom.

(v) Public dissemination of types and frequency of surveillance. Standard 2-9.1(f)(v) calls for "maintaining and making available to the public general information about the type or types of surveillance being used," as well as the "frequency of their use." This standard recognizes that public awareness about the extent of government surveillance can be a powerful accountability mechanism. Precedent for such disclosure is found in the communications surveillance context, where annual disclosures about the

extent of electronic surveillance are mandated by Title III.[71] This disclosure has not interfered with law enforcement. At the same time, it has kept the public abreast of how the government is conducting its investigations and the extent to which it relies on technology.

The provision is not meant to require revelation of specific government technologies, as it makes clear in providing that "sensitive law enforcement information need not be disclosed." But the standard is designed to keep the public apprised of the general reach of those technologies. Thus, it contemplates that government will periodically release information as to the approximate number and length of surveillances using video technology, and tracking, telescopic, illumination, and detection devices. Such information should be relatively easily compiled if, as called for in Standard 2-9.1(f)(i), documentation is maintained.

Standard 2-9.1 General Principles

(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 2-9.3 through 2-9.6;

(ii) the rules developed by other agencies pursuant to Standard 2-9.1(e); and

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

---

71. 18 U.S.C. § 2519(3).

Commentary to Standard 2-9.1(g)

The importance of Standard 2-9.1(g) cannot be overstated. As the commentary to the ABA Standards Relating to the Urban Police Function explained,[72] any meaningful regime of police regulation must include an administrative component. Especially as to standards of conduct which are not subject to exclusionary sanctions, and which consequently never receive attention from judges, elaboration is needed via the administrative process.

Individual officers cannot be expected to work everything out for themselves in these situations. Instead, departments should develop policies which translate the general principles in this standard, and the specific rules in the standards which follow, into detailed guidelines for various forms of physical surveillance. Standard 2-9.1(g) makes clear that such administrative rules should be adopted, and that they should include both "written instructions regarding resort to regulated technologically-assisted physical surveillance" and a "mandate that officers of that agency comply with those instructions."

Standard 2-9.1 General Principles

(h) *Non-binding effect of standards.*

Nothing in these standards is intended to create rights, privileges, or benefits not otherwise recognized by law. Rather, they are meant to ensure that surveillance decisions are based on all relevant considerations and information.

---

72. *See* commentary to ABA Standards Relating to the Urban Police Function 116-44 (1st ed. 1973).

Commentary to Standard 2-9.1(h)

The purpose of Standard 2-9.1(h) is to emphasize, once again, that these standards are not intended to encourage the courts to expand (or contract) current Fourth Amendment jurisprudence, or to create additional "rights, privileges, or benefits" not otherwise recognized under Fourth Amendment case law.[73] Rather, this standard provides that the purpose of these standards is to ensure that in making "surveillance decisions," courts, legislatures, and administrative bodies are aware of "all relevant considerations and information." These standards leave to the appropriate bodies the remedies, if any, to be attached to violations of those rules.

Standard 2-9.2 Definitions

The following definitions apply to Standards 2-9.3 through 2-9.6:

(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 *contraband-specific* if it can only reveal the presence of an object that 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 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"

---

73. *See also* Standard 2-9.1(f)(ii) (concerning availability of exclusionary sanction).

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 area where it occurs or exists and other relevant considerations 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.**

Commentary to Standard 2-9.2

Standard 2-9.2 defines key terms that are used in the standards governing specific categories of surveillance devices, *i.e.*, Standards 2-9.3 through 2-9.6 (concerning, respectively, video surveillance, tracking devices, illumination and telescopic devices, and detection devices).

(a) Covert surveillance

Standard 2-9.2(a) defines "covert surveillance," while the related concept of "overt surveillance" is defined in Standard 2-9.2(e). 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 is required for certain types of covert surveillance (*see* Standard 2-9.1(d)(v)(B)). Covert video surveillance is not regulated as strictly as long term overt video surveillance (*compare* Standard 2-9.3(b) *with* Standard 2-9.3(c)). Brief overt use of telescopic and illumination devices to view non-private activities is not regulated at all, while covert use of these technologies is regulated (*see* Standard 2-9.5(b)). Thus, a definition of "covert" surveillance is necessary. Standard 2-9.2(a) defines this term to mean surveillance that is "intended to be concealed from any subject of the surveillance."

(b) Detection devices

Standard 2-9.2(b) defines a detection device as a device that allows users to "detect the presence" of particular objects or characteristics through "opaque inanimate barriers" such as clothing and walls. Thus, this definition specifically excludes devices that can detect microscopic or transparent particles (*e.g.*, cocaine, fluids, or fingerprints) that are invisible to the naked eye even when no barrier between the items and the eye exist. Use of the qualifier "inanimate" is meant to exempt from the purview of these standards devices such as breathalyzers or x-rays which permit detection of the contents of one's body. Government use of the latter devices is not easily labeled "surveillance" and in any event is already governed by a significant body of case law.[1]

Several different types of detection devices exist or are on the verge of production. One example of the type of technique contemplated by this definition registers the degree of radiation emitted from the body and objects

---

1. Skinner v. Railway Labor Executives' Assoc., 489 U.S. 602 (1989) (blood and breath drug tests); National Treasury Emp. Union v. Von Raab, 489 U.S. 656 (1989) (urinalysis drug testing). *Cf.* Montoya de Hernandez, 473 U.S. 531 (1985) (avoiding a decision about use of x-rays to determine whether drugs have been swallowed); Winston v. Lee, 470 U.S. 753 (1985) (requiring heightened scrutiny of surgery to detect evidence of crime).

concealed on it. Because these waves readily pass through clothing, and because the body is a good "emitter" while metal and other dense, inanimate objects tend to be bad "emitters," the latter objects show up on the device as outlines against the body. Another example is a device which aims a low intensity electromagnetic pulse at the subject and measures the time decay of each object radiated, a period which differs depending upon the object. The device then compares the time-decay of the object with known "signatures" of items like guns; no image is produced. A third example is a device which measures the fluctuations in the earth's magnetic field produced by ferromagnetic material (like the metal in a gun) which moves through it.[2] A fourth illustration is the panoply of thermal imaging devices which measure the "heat waste" emitted from behind opaque barriers.[3] This definition encompasses all of these devices, whether they are passive (as with the radiation and thermal imaging devices) or active (as with x-rays), and whether they produce an image of the object (as with the radiation device) or simply register the presence of an item or a characteristic.

This definition also recognizes that detection devices may detect only contraband ("contraband-specific"), only weapons ("weapon-specific"), or a variety of hidden objects in addition to contraband and weapons (what this Commentary will call a "general detection device"). Most devices are of the latter variety. For instance, an x-ray of a container may reveal not only a gun, but also the outline of other stored items. A magnetometer at an airport reveals not only the presence of a weapon but of keys, coins, and other metallic objects. These devices would not be contraband- or weapon-specific, either because they identify noncontraband as well as contraband or because they do not clearly identify an object as either. On the other hand, a device which could mimic the behavior of some specially trained dogs by alerting only to the presence of drugs would be "contraband-specific." A

---

2. For a description of these devices, see David A. Harris, *Superman's X-Ray Vision and the Fourth Amendment: The New Gun Detection Technology*, 29 TEMPLE L. REV. 7-8 n. 38 (1996).

3. One such device looks like a 35 millimeter camera, has a range of up to 400 meters, and can detect temperature differences as small as one-half a degree. Matthew L. Zabel, *Thermal Imagery vs. the Fourth Amendment*, 90 NW. U. L. Rev. 267, 269 (1995).

device which detected only the presence of guns would be "weapon-specific."[4]

The specific-nonspecific distinction is important in light of case law which suggests that the Fourth Amendment is not implicated by a police action which detects only contraband.[5] As Standard 2-9.2(b) recognizes, whether something is "contraband" will depend upon whether the item is "virtually always criminal to possess or use in the existing circumstances." Carrying drugs like marijuana and cocaine is virtually always criminal. Concealing a weapon, on the other hand, may not be. Possessing a weapon is virtually always criminal if it occurs at an airport, and concealing a gun is usually criminal in states which limit who can do so to a small group of people (usually law enforcement officials and similar professionals). But in states where carrying a concealed weapon is legally permissible, a device which detected only guns would generally not be a contraband-specific device under this definition. Such a device would be weapon-specific, however, a distinction which becomes important in Standard 2-9.6 in defining when detection devices may be used for protective purposes.

(c) Illumination devices

Standard 2-9.2(c) defines illumination devices broadly. It is not limited to those devices that literally "illuminate" targets, but encompasses any device which permits viewing in darkness. For instance, infrared technology used in many types of nightscopes allow nightvision in low-light conditions without any telltale illumination that would give the observer away.[6] These devices can be held in one hand, obtain high resolution, come with a photo

---

4. The injunction in Standard 2-9.1(d)(iv) that investigative technology be scientifically validated for what it purports to do is especially important here. If a device purports to detect guns, but is inaccurate 50% of the time, then it would not qualify as a contraband- or weapons-specific device.

5. *Cf.* United States v. Place, 462 U.S. 696 (1983); United States v. Jacobsen, 466 U.S. 109 (1984).

6. ITT Electro Optics Product Division, Night Enforcer 250, ITT Vision Equipment (Abstract presented at National Institute of Justice Law Enforcement Technology Program, May 15, 1995).

capacity, and prevent "blooming" when bright light sources are encountered. They can also be equipped with telescopic capacity.[7]

(d) Legitimate law enforcement objective

Standard 2-9.2(d) defines the phrase "reasonably likely to achieve a legitimate law enforcement objective." This phrase is particularly critical in the standards which follow because, with only a few exceptions, it describes when technologically-assisted physical surveillance of a nonprivate area, activity, or condition may take place. In other words, this term establishes the standard the police must meet in those situations not regulated by the Fourth Amendment.

Because neither courts nor legislatures have focused their attention on these situations, the "reasonably likely to achieve a legitimate law enforcement objective" language introduces a new regulatory concept. As defined in this standard, the concept requires that there be "articulable reasons for concluding that [legitimate law enforcement] objectives may be met by taking the action." The concept has two essential elements.

First, the reference to "legitimate law enforcement objectives" incorporates the general principle in Standard 2-9.1(a) that all surveillance should be for the "detection, investigation, deterrence or prevention of crime or apprehension and prosecution of a suspected criminal." If there are "articulable reasons for concluding that one of these objectives may be met by taking the action," then the action has a legitimate law enforcement objective. On the other hand, surveillance for ends that cannot be articulated in these terms (*e.g.*, surveillance that is clearly for political or harassment purposes only) would not be for a legitimate law enforcement purpose. Because the definition only requires that legitimate reasons be "articulable," however, it leaves unresolved whether surveillance that is ostensibly for a

---

7. For a general description of many of these devices, *see* 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, at 678 (1988) and accompanying notes.

legitimate purpose may in fact be for an illegitimate one (so-called pretextual actions).[8]

The second essential element of the phrase is the "reasonably likely" criterion, which in turns depends upon what is meant by the term "articulable reasons." At first glance, the latter term may appear to encompass the reasonable suspicion standard defined in *Terry v. Ohio*,[9] which requires "specific and articulable" facts as the basis for a stop or frisk. Note, however, that what is required here is not a finding that a particular person will be tied to the crime (which would equate with an individualized suspicion requirement), but rather articulable reasons why 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 surveilled, but they may well have an articulable reason for believing that, if covert, the videotape will help accomplish an investigatory end or, if overt, a deterrent end. Or police may want to use binoculars to surveil, without being discovered, an area known for dangerous drug trafficking. Again, there is 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 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"/"articulable reasons" language does require that the police's objectives be specifiable.[10] Monitoring of innocent activity that has no explicable relationship to investigatory, deterrent or protective purposes does not meet this definition. Generally speaking, investigatory objectives should be driven by a *particular* offense or type of offense, rather than a generalized concern about crime, and deterrence

---

8. In Whren v. United States, 116 S.Ct. 1769 (1996), the Supreme Court held that police actions based on a probable cause belief that a violation of the law has occurred are not unconstitutional simply because police had a hidden illegitimate agenda, but left open whether the Fourth Amendment is violated by pretextual actions when probable cause is not present (which is the case here).

9. 392 U.S. 1 (1968).

10. Recall also that Standard 2-9.1(f)(i) suggests that, under some circumstances, the articulable reasons be documented.

objectives should be associated with a desire to deal with a *demonstrable* crime problem.

In short, the definition of which police objectives are legitimate (*i.e.*, investigation, deterrence, prevention, protection of crime and apprehension of criminals) and the definition of how likely the achievement of those objectives has to be (*i.e.*, when there are articulable reasons) is meant to provide meaningful but not onerous limitations on police conduct.

(e) Overt surveillance

While Standard 2-9.2(a) defined "covert surveillance," Standard 2-9.2(e) defines "overt surveillance." As noted, the distinction between overt and covert surveillance is important in connection with several of these standards. Standard 2-9.2(e) endorses an objective definition of overt surveillance (surveillance "of which a reasonable person would be aware") so as to include surveillance that is clearly overt, even if those surveilled do not happen to notice it. However, surveillance that law enforcement *intends* to go unnoticed by those surveilled would be covert, as defined under Standard 2-9.2(a).

(f) Private

Standard 2-9.2(f) defines "private," another crucial term in the specific standards that follow. As used in those standards, the word "private" is a term of art designed to indicate which situations implicate the Fourth Amendment and thus trigger the warrant and probable cause requirements. As explained earlier, these standards do not seek to expand the scope of Fourth Amendment protection. Thus, this standard defines "private" to mean a place, activity, condition, or location that would have a "constitutionally reasonable expectation of privacy," in order to ensure that this term is coextensive with Fourth Amendment usage.

The second sentence of this definition states that, where these 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 these standards (in connection with tracking and detection devices), houses, luggage and so on are entitled to full Fourth Amendment protection regardless of the sophistication of the device used, the steps taken

to ensure privacy, and similar types of considerations. The reasons for this distinctive treatment are discussed in connection with the relevant standards.

(g) Reviewing law enforcement official

Standard 2-9.2(g) defines a "reviewing law enforcement official" to mean an officer "other than the person who will implement the surveillance." This definition implements the concept alluded to in connection with Standard 2-9.1(e), which recognizes that where administrative decisionmaking about physical surveillance is involved, multiple levels of decisionmaking authority should be recognized. At a minimum, there are three such levels: the surveilling or field officer and the two levels of "reviewing" officials recognized in this standard.

The first level of review recognized in the standard is the "supervisory" official (*e.g.*, a sergeant, lieutenant, or captain). The second is a "politically accountable" official (*e.g.*, the head of a police department or a district attorney), who will normally be politically accountable either through the election process or because his or her appointment is dependent upon a person who is elected. Given the diversity of command structures, it would be unwise to attempt any greater specificity here. But these three basic distinctions are crucial for differentiating the nature of administrative decisionmaking about technologically-assisted physical surveillance.

(h) Telescopic devices

Standard 2-9.2(h) defines telescopic devices to mean any device that "makes visible details not visible to the naked eye because of distance." This definition includes devices which permit viewing over a distance but excludes items, like microscopes, which magnify infinitesimal particles. Further, the definition includes not only "real-time" magnification, but enlargement of a picture after it is taken. In other words, this definition is meant to govern technology that allows subsequent, as well as contemporaneous, enhancement of vision.

(i) Tracking devices

Standard 2-9.2(i) defines tracking devices to mean "devices used to track movement of persons, effects, or vehicles." As noted in the introduction to these standards, such devices may include beepers and "intelligent

transportation systems" ("ITS"). The former device is planted on the object sought to be traced and sends electronic signals to a transponder which can pick up those signals over a certain range. An ITS (sometimes called an IVHS, for "intelligent vehicle highway system") in effect involves installing a beeper in every car, except that the available range could be much greater, depending upon how pervasive the transponder network is.[11] Also under development for law enforcement use are radars that can detect objects beyond the earth's horizon and that can transform the two-dimensional radar image into a three-dimensional one.[12]

Tracking need not rely on installation of a device, however, or even on aiming a device at the intended target. Tracking the signals from a cellular phone already in a car would fall under this definition as well. Similarly, one version of the bistatic tracking device mentioned in the introduction to these standards is capable of ground or airborne surveillance using existing sources of illumination to provide a tracking capability.[13] Another more exotic tracking device is a radar-type mechanism used by the military to trace chemicals sprayed on food meant to be eaten by the target of the surveillance.[14]

(j) Video surveillance

Standard 2-9.2(j) defines video surveillance to mean the "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 who is aware of the use. This definition is meant to exclude from the ambit of "video surveillance" camera shots that merely replicate what an officer on the scene can see for himself or herself. Thus,

---

11. *See* Dep't of Transportation, *National Program Plan for Intelligent Transportation Systems* (Final Draft, Nov. 1994).

12. Dep't 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).

13. Dep't 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).

14. TIME, August 21, 1995, at 41.

cameras in police cruisers or on uniform lapels would not constitute video surveillance for purposes of these standards.

The requirement that the camera be "lawfully positioned" is included to ensure that video surveillance of private activity using an unlawfully placed video camera does not escape regulation simply because the activity is also viewed by an officer or undercover agent. Standard 2-9.3(a) deals with the circumstances under which a video camera that views a private activity or condition may lawfully be installed.

Standard 2-9.3 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 2-1.1 et seq.], as modified for video surveillance.

(b) Overt video surveillance for a protracted period not governed by Standard 2-9.3(a) is permissible when:

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

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

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

(ii) in cases where deterrence rather than investigation is the primary objective, 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 2-9.3(a) or (b) is permissible when a supervisory law enforcement official, or the surveilling officer when there are exigent circumstances, concludes that the surveillance:

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

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

Commentary to Standard 2-9.3

Standard 2-9.3, governing video surveillance, is divided into three subsections. Standard 2-9.3(a) governs the use of video surveillance to view a "private activity or condition." Standard 2-9.3(b) governs the use of "overt" video surveillance to view a public place for a "protracted period." Standard 2-9.3(c) is a catch-all provision that governs the use of video surveillance in other circumstances, *i.e.*, the use of "overt" video surveillance for short periods to view public, non-private activities and places and the use of covert video surveillance to view such activities and places.

(a) Video surveillance of private activities or conditions

Under Standard 2-9.3(a), the rules regarding video surveillance of "private" activities and conditions are identical to those governing aural surveillance, which are set out in the Electronic Surveillance chapter of the ABA Criminal Justice Standards (Standards 2-1.1 through 2-5.17), and incorporated by reference. The latter standards, in brief, require a judicially-authorized warrant, based on probable cause, before interception of private communications may take place.

The caveat in Standard 2-9.3(a) that the aural surveillance standards be "modified for video surveillance" is merely meant to alert the reader to the obvious point that references to concepts such as "acquisitions of communications" must be changed to "viewing of activities and conditions" to make them relevant to video surveillance. After making these conforming modifications, the key effect of this standard is to require that video surveillance of private activities and conditions be conducted with a warrant, unless there is consent or an emergency.

Most courts have adopted the equation of aural and video surveillance incorporated in this standard. The leading case in this regard, *United States*

v. Torres,[1] held that, while Title III does not deal with video surveillance, its provisions could be applied by analogy. Thus, according to *Torres*, a Title III warrant describing with particularity the place to be viewed is necessary to authorize such surveillance, and may issue only if other means of investigation have failed and steps are taken to minimize unnecessary privacy intrusions. Several other courts have agreed with *Torres*.[2]

A number of commentators, however, have argued that video surveillance ought to be more strictly regulated than aural surveillance. For instance, it has been suggested that: (1) video surveillance should be authorized for fewer types of crimes than is the case with aural surveillance; (2) video surveillance should be permitted only if aural surveillance first indicates criminal activity is occurring; (3) video surveillance should be permitted only if the judge identifies the person to be surveilled (which is only required for aural surveillance if the person is known); (4) the court order for video surveillance should be of shorter duration; and (5) warrantless video surveillance ought to be prohibited even when one of the parties consents to it.[3] None of these suggestions is adopted here, on the ground that, at least in theory, video surveillance is often no more intrusive and may sometimes be less intrusive than aural surveillance.

The Standards Committee does not reject the possibility that, under some circumstances, video surveillance of private activities and conditions should

---

1. 751 F.2d 875 (7th Cir. 1984).

2. *See, e.g.*, United States v. Falls, 34 F.3d 674 (8th Cir. 1994); United States v. Koyomejian, 970 F.2d 536 (9th Cir. 1992). However, a few courts have applied only those aspects of Title III to video surveillance which they believe are required by the Fourth Amendment, meaning, for instance, that the provisions of Title III which require applications to be signed by certain types of prosecutors and which limit surveillance to certain crimes do not apply. *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 criticisms of these cases, *see* Kent Greenfield, *Cameras in Teddy Bears: Electronic Visual Surveillance and the Fourth Amendment*, 58 U. CHI. L. REV. 1045 (1991); Note, *Let's Go to the Videotape: The Second Circuit Sanctions Covert Video Surveillance of Domestic Criminals*, 53 BROOKLYN L. REV. 469 (1987).

3. *See* Greenfield, *supra* note 2, at 1045 et. seq.

be regulated differently than aural surveillance of private communications.[4] However, the Committee decided that the need for any differential treatment could best be addressed in connection with revising the Electronic Surveillance Standards, which are currently being considered for their third edition. Any changes made in those standards as a result of that review process are intended to be incorporated by reference in these standards as well. In the meantime, the Second Edition Electronic Surveillance Standards and commentary thereto should provide guidance as to how Standard 2-9.3(a) is intended to apply with respect to video surveillance of private activities and conditions.

This general observation notwithstanding, one interpretative anomaly produced by the equation of the video and aural surveillance standards must be noted. Standard 2-3.3(c) of the current communications standards provides that, before a court may issue a warrant authorizing acquisition of private communications, it must find probable cause to believe that "other investigative procedures have or had been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous." Because video surveillance is an "investigative procedure," the cross-reference to this provision in this standard could produce the absurd consequence of prohibiting both aural or video surveillance in any case where either is "likely to succeed" at obtaining the evidence. To avoid this result, the standard should be read to permit either type of surveillance if there is probable cause to believe other investigative procedures are likely to fail or are too dangerous. In its revisions of the communications surveillance standards, the Committee may consider whether there should be a preference

4. For example, Standard 2-2.1 of the Second Edition Electronic Surveillance Standards recommends legislation criminalizing the "possession, sale, distribution, advertisement, or manufacture" of interception devices, a prohibition which presumably could not be meaningfully transferred to the physical surveillance context, given the prolific use of binoculars, flashlights and so on. As another example, Standard 2-5.1 of the Second Edition Electronic Surveillance Standards provides that "a law enforcement officer should be permitted to acquire a private communication surreptitiously with the consent of one of the parties to the communication without the necessity of a court order . . . ." This standard as applied to video surveillance might be construed to require the presence of the consentor during the entire video surveillance; whether that result is appropriate has not been resolved by the Committee.

for one type of surveillance over another, but no judgment about this issue is made at this time.

(b) Long-term public video surveillance

Standard 2-9.3(b) governs the use of "overt" video surveillance for a "protracted period," when used to view *non*private activities or conditions. The presence of video cameras, steadily panning the city streets, directly compromises the desire and ability to remain anonymous in one's comings and goings. The feeling of unease that conspicuously-positioned video cameras may create is likely to be particularly acute when the cameras are permanent and designed to monitor everyone in the area, at all times of the day.

Yet such cameras can also identify culprits and gather information about suspicious activity or groups of people. Further, cameras facilitate law enforcement by providing accurate documentation of crimes when there are no witnesses and facilitating interviewing the witnesses when they exist. These capacities are augmented further when a "zoom" capacity, in real-time or subsequent to the event, is available to magnify what is monitored. Law enforcement and the public should not be deprived of this crime-fighting mechanism if its use can accommodate privacy and related concerns.

Accordingly, Standard 2-9.3(b) permits long-term overt video surveillance when a politically accountable government entity concludes that it will "not view a private activity or condition" and is "reasonably likely to achieve a legitimate law enforcement objective." As noted, the latter term is defined in Standard 2-9.2(d) to require "articulable" reasons for concluding the surveillance will further investigative, deterrent, or protective aims. In other words, if such surveillance can possibly resolve a known crime problem, it may be pursued. If instead it is used merely as an easier way of randomly spying on the general populace, it should not be.

To illustrate, the showing required by Standard 2-9.3(b) would be met if the targeted area is demonstrably crime-ridden, or has experienced a spate of street crimes or traffic violations. Overt video monitoring of the public space in front of a federal building or at an international sporting event might also meet the test established by this standard; even if no threat has been made against the particular building or event, the fact that serious threats have been made in similar contexts may well justify the protection and deterrence

afforded by such surveillance. In contrast, suppose police want to set up cameras at a series of street corners not because numerous crimes have occurred at these locations, but because the recordings the cameras produced might be useful in a future investigation of some unidentified crime. Such surveillance would not be permitted under this standard.

Because this type of surveillance is both overt and long-term, this standard does not rest the decision about conducting such surveillance with the surveilling officers or even with their immediate supervisor. Standard 2-9.3(b)(i) instead requires substantial agency and public input. First, either a "politically accountable" law enforcement official, a term defined in Standard 2-9.2(g), or the relevant elected governmental body or its delegate (*e.g.*, a commission) must determine that a legitimate law enforcement objective is likely to be achieved. Second, when "deterrence rather than investigation is the primary objective," Standard 2-9.3(b)(ii) requires that the public have a direct opportunity to learn about, and give feedback regarding, the intended surveillance.

The requirement that a high-level law enforcement official or an accountable government body be involved in the decision to set up public video surveillance is important for a number of reasons. First, these decisionmakers are more representative of the public than is a supervisor or field officer. In addition, a decision which is likely to affect large numbers of people for a long period of time should not be made by a low-level official, regardless of the latter's expertise and knowledge of local conditions. Finally, only at the departmental level are the relevant statistics necessary for documenting a crime problem likely to be available.

Although the involvement of politically accountable officials allows for indirect public input, the public is given an opportunity to register its concerns more directly because, both from a philosophical and practical standpoint, government searches which affect large groups of people should be mediated through the political process. If the public is involved in approval of the surveillance it is more likely to understand its nature and purpose and any sense of discomfort associated with it is likely to be minimized. Note, however, that the standard limits public involvement to those "to be affected by the surveillance." This group would include those who live in or frequent the area to be surveilled, but generally would not

include the public at large, which might be insensitive to the intrusion represented by mounted cameras in someone else's neighborhood.

Consistent with Standard 2-9.1(d)(v)(A) of the general principles, this standard also provides that the "public to be affected" be notified of the surveillance once it is in place (presumably through signs, etc.). Obviously, there will be little deterrence if there is no notice. Notice is also important as a privacy protection measure. People should know about the placement of the cameras so they can avoid them if they choose.

Standard 2-9.1(f)(iv) of the general principles requires that the efficacy of all technologically-assisted physical surveillance be reviewed periodically. For public video surveillance, that review should include an assessment of whether the surveillance does in fact deter crime. As one way of implementing that goal, Standard (b)(ii)(B) includes the requirement that the public be 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," whether through a hearing or other means. Perhaps the most probative information in this context is how citizens perceive the camera's effects both on the crime rate and on their own privacy and interest in anonymity.

Although Standard 2-9.1(c)(iv) of the general principles encourages use of the least restrictive means of accomplishing the government's goals, this standard does not require attempts at other crime-deterrence steps before initiation of public video surveillance. While putting an officer on every corner might be just as effective a video camera system, it is not clear that such procedures are less intrusive. The fact that such steps have been taken and failed, however, might make public video surveillance more palatable to the affected public.

This standard is also intended to be read in conjunction with Standard 2-9.1(d)(vii) of the general principles, which directs as a further precaution against misuse that protocols be developed concerning the maintenance and disposition of such recordings. Police departments, perhaps working with prosecutors, should enact regulations detailing precisely how such maintenance should take place and for how long. In some jurisdictions, for instance, regulations require that video recordings from street cameras be

destroyed shortly after their creation (*e.g.*, 96 hours) if no law enforcement use for them becomes apparent within that time.[5]

(c) Other video surveillance of public activities

Standard 2-9.3(c) governs both covert and "short-term" overt video surveillance of public places, neither of which fall within the prior video surveillance provisions. Both types of surveillance can fulfill important law enforcement objectives. Covert video surveillance of public areas might be considered when police know a particular area is crime-ridden, but have had difficulty, using overt methods, discovering who is committing the crimes. Similarly, such surveillance might be useful when police have reason to believe a crime will be committed in certain types of public areas (*e.g.*, because of a recent string of pawn shop burglaries), but they do not know when it will occur. Short-term overt surveillance of public places could, in theory, also allow the police to identify perpetrators who either forget about or ignore the cameras. However, it is more likely to be used for the same purposes as long-term overt video surveillance: information-gathering, and deterring crime by conspicuously asserting a government presence in a particular area.

Standard 2-9.3(c) provides that either type of surveillance is permissible when it "will not view a private activity or condition," and when it "will be reasonably likely to achieve a legitimate law enforcement objective." As discussed in connection with long-term video surveillance, a documented series of crimes within the area sought to be surveilled would meet this threshold test, while a showing of only one or two unrelated crimes normally would not. In short, while the standard permits efforts to solve, deter or protect against specified crimes or types of crimes, it prohibits the monitoring of innocent activity or conditions having no articulable relationship to any reasonably anticipated offense.

Given the fact that large groups of people are often targeted by video surveillance of nonprivate activities, this standard provides also that, in most cases, such surveillance should be approved by a "supervisory law enforcement official." However, where there are "exigent circumstances,"

---

5. *See supra* note 61, Standard 2-9.1(d)(vii).

the standard recognizes that the determination may legitimately be made directly by the surveilling officer.

Because the targets of covert video surveillance do not know they are being watched and thus may not take precautions against revelation of private and intimate activities, it could be argued that individualized suspicion and judicial authorization should be required for this type of surveillance, at least when it is long-term. However, by choosing to carry out the activity in a public place, a person knowingly increases the chances of being viewed by someone else. Furthermore, a requirement of individualized suspicion would defeat the usual purpose of covert video surveillance, which is to identify who is committing a crime or crimes the police suspect will take place.

As with all specific types of surveillance governed by these standards, the general principles set forth in Standard 2-9.1 apply here. Covert and short-term overt surveillance must be limited in scope and duration to achievement of the authorized objective, and cannot be implemented in a discriminatory fashion (*see* Standards 2-9.1(d)(ii)). There are also limitations, previously noted, concerning the subsequent destruction of recordings made during video surveillance and, as provided in Standard 2-9.1(d)(vi), disclosure and use of the recordings may occur only "for lawful designated purposes."

With respect to short-term overt surveillance only, an additional consideration arises. Standard 2-9.1(d)(v)(A) provides that pre-surveillance notice should be given "when deterrence is a goal or when persons should be given the opportunity to avoid the surveillance." In light of this standard, some type of notice of short-term overt surveillance should be considered. If, for instance, police wish to film a rally, notifying the organizers of the rally or running an announcement in the local newspaper should be contemplated. Potential attendees who would rather not appear on a police tape should know about the cameras in advance.

Standard 2-9.4 Tracking Devices

(a) Installation pursuant to paragraph (b)(i) and monitoring pursuant to paragraph (c)(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

it shall be obtained 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.

(b) 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.

(c) 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 sufficient basis under applicable constitutional principles to believe that such monitoring will reveal evidence of crime, provided that, if one or more of the subjects of the monitoring consents to have the tracking device accompany their person, 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.

Commentary to Standard 2-9.4

Standard 2-9.4 governs the use of tracking devices. It is divided into three subsections: Standard 2-9.4(a) addresses the circumstances under which a court order is needed for installing or monitoring a tracking device (and the

exceptions to that requirement); Standard 2-9.4(b) concerns the requirements for installing a tracking device; and Standard 2-9.4(c) concerns the requirements for monitoring a tracking device. The standard makes a fundamental distinction between conducting such surveillance within a private location and tracking suspects in public spaces.

(a) Court order

Standard 2-9.4(a) addresses the need for "written authorization by a judicial officer." Such authorization is required by Standard 2-9.4(b)(i) when installation of a tracking device involves "entering a private place without consent" and by Standard 2-9.4(c)(i)) before monitoring a tracking device to determine "where it is located within a private location." The standard requires a court order in these situations, except where exigent circumstances make it unfeasible to obtain such an order in advance, in which case court authorization must be obtained "as soon as practicable" thereafter.

The requirement for a court order to *monitor* a tracking device within a private location finds support in the Supreme Court's holding in *Karo v. United States*[1] that judicial review is necessary if a tracking device is used to detect movement inside a home. Whether the Fourth Amendment requires a warrant before *installation* of a tracking device in a private place is not quite as clear. In *Dalia v. United States*[2] the Supreme Court held that Title III does not require a separate warrant for installation of electronic surveillance equipment within a home.[3]

However, in cases like *Dalia* the installation is preceded by a judicial finding that the house in which the installation took place contained communication devices likely to be used for criminal activity. In contrast, a judicial finding that a car or object may be tracked does not reflect any kind of judgment about the garage or house the police plan to enter in order to affix the device. Thus, Standard 2-9.4(a) provides that a court should address the constitutionality of installations as well as monitoring of tracking devices within private areas.

---

1. 468 U.S. 705 (1984).
2. 441 U.S. 238 (1979).
3. *Id.* at 258.

This standard also places a durational limitation on the surveillance. It provides that the court order should authorize such surveillance only for "as long as necessary to achieve the authorized objective[s]" and no longer than a maximum of 60 days unless there are "articulable facts demonstrating a need for longer surveillance." Extensions of 60 days are permitted on reauthorization by the judge under the appropriate standard.

As *Karo* indicated,[4] without such a durational limitation the surveillance becomes an extreme intrusion, potentially amounting to months of surveillance justified solely—at least in appearance—by the mere hope that useful information will be produced. The 60-day time period provided for is identical to the durational limitations on court orders for pen registers under the federal Electronic Communications Privacy Act.[5] However, it is twice as long as the duration of warrants for communications surveillance under relevant federal law and four times as long as communications and video surveillance warrants authorized under these standards.[6] Because long-term use of tracking devices is relatively common, sometimes involving waits of a month or longer before the device indicates any movement,[7] the shorter terms were rejected as unduly burdensome to law enforcement.

The conclusion that long-term tracking can be inimical to individual interests might also argue for durational limitations when the tracking occurs solely in public places. Although the standard places no time limit on this type of surveillance, as a practical matter the 60-day period in this provision is likely to apply in any case involving more than a day of tracking. Because of the great likelihood 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.

---

4. 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. 468 U.S. at 718.

5. 18 U.S.C. § 3123(c)(1).

6. 18 U.S.C. § 2518(5) (30 days); ABA Criminal Justice Standard 2-5.8(j) (15 days).

7. This was the assertion of several federal law enforcement officials who either served on or gave presentations to the Task Force on Technology and Law Enforcement.

(b) Installation of tracking devices

Standard 2-9.4(b) concerns the installation of tracking devices, except when installation is "part of a systemwide program authorized by the legislature." It is basic Fourth Amendment law that entering a private place, without consent,[8] requires probable cause to believe evidence will thereby be acquired. There is no reason to vary this rule because the means of obtaining that evidence is a tracking device rather than the traditional search. Thus, Standard 2-9.4(b) recognizes that installation which requires entering a private place without consent requires probable cause to believe that "the object to be tracked is at the location to be entered" and that "subsequent monitoring of the device will reveal evidence of crime" (as well as a court order in the situations described in Standard 2-9.4(a)).

In all other situations where nonconsensual installation of a tracking device is necessary, this standard requires simply that subsequent monitoring of the device be "reasonably likely to achieve a legitimate law enforcement objective." Although installation in this latter situation does not infringe any reasonable expectation of privacy, the fact that the device will eventually be used to track movements necessitates some limitation.

The reference to systemwide programs authorized by the legislature is meant to exempt "intelligent transportation systems" from the purview of this provision. Such systems involve government installation of tracking devices in every car within a given transportation network, which obviously could not be based on probable cause or any type of suspicion. This standard takes no position on the constitutionality or propriety of such a system. However, if a monitoring capability were included as part of such a system, law enforcement use of the device to track a particular car would still have to meet the monitoring requirements under Standard 2-9.4(c), described below.

---

8. Consent, of course, vitiates a Fourth Amendment claim. In United States v. Karo, 468 U.S. 705 (1984), the Supreme Court held that installing a beeper in an ether can with the owner's consent, before it is delivered to the person to be tracked, is not a seizure (since the installation does not result in dispossession of any property) or a search (since no expectation of privacy is violated by the presence of an inactivated beeper).

(c) Monitoring of tracking devices

Standard 2-9.4(c) governs the circumstances under which monitoring a tracking device is permissible. Constitutional doctrine concerning use of tracking devices once they are installed derives largely from two United States Supreme Court cases.[9]

In *United States v. Knotts*,[10] 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. In contrast, in the *Karo* decision,[11] the Court held that 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, *Karo* also held that 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 as yet unknown.[12] Furthermore, the Court left open whether reasonable suspicion (as opposed to probable cause) is sufficient to authorize the warrant.[13]

Because the latter issue has not been resolved by the Court, Standard 2-9.4(c) simply provides that monitoring a tracking device to determine whether, or where, it is located within a private location[14] is permissible

---

9. Title III mentions tracking devices, but does not seriously regulate them, merely providing (in a 1986 amendment) that "if 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 the jurisdiction if the device is installed in that jurisdiction." 18 U.S.C. § 3117(a). This provision allows beepers authorized in one jurisdiction to be used in other jurisdictions.

10. 460 U.S. 276 (1983).

11. 468 U.S. 705 (1984).

12. *Id.* at 718.

13. *Id.* at 718 n.5.

14. Note that the word "location" is used in the standard, rather than the word "place." As defined in Standard 2-9.2(f), a private place is one which, if entered physically, would be protected by a constitutionally protected reasonable expectation of privacy. It is possible, however, 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 was recognized in *Karo*, when it stated that 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.

when there is "sufficient basis under applicable constitutional principles to believe that such monitoring will reveal evidence of crime." Use of the phrase "applicable constitutional principles" is intended to leave to the courts resolution of whether probable cause or reasonable suspicion is required in this situation.

Where the tracking device is used instead to track within public space, Standard 2-9.4(c)(ii) only requires that there continue to be "a reasonable likelihood that such monitoring will achieve a legitimate law enforcement objective." The Supreme Court observed in *Knotts* that travel in public is easily observable and chose not to bring such travel within the purview of the Fourth Amendment.[15] Thus this standard does not require reasonable suspicion or probable cause for monitoring such public travels.

For reasons already noted, however, the cautious law enforcement officer should probably obtain a court order even when private entry for installation purposes is not necessary and only public monitoring is anticipated. It is rarely known ahead of time when a tracking device might end up inside a house or similar location. Of course, nothing in this standard prevents police with only a legitimate law enforcement objective in mind from using a device to publicly track an item *to* a particular house. However, if, as occurred in both *Knotts* and *Karo*, the signal on a beeper is temporarily lost, *Karo* would require a greater degree of cause to relocate the signal in a private place. Such cause would also be required if public tracking leads the police to an apartment building or a conglomeration of buildings, so that identifying the precise apartment or building in which the item is located is impossible without resort to the tracking device. For these reasons, seeking an order may often be the safest course.

Several factors mitigate law enforcement's burden in that regard, however. First, as *Karo* held, precisely because the destinations of the device are not known, the cause required here focuses solely on the likelihood that evidence will be discovered; the place ultimately to be searched need not be stated with particularity. Second, if the device is installed in an item containing contraband (such as the ether can involved in *Karo*), such cause will generally readily be found because, once acquired, the item's carrier is

15. 460 U.S. at 282.

committing a crime. Third, Standard 2-9.4(a) sets out an exigency exception to the court order requirement, which would apply whenever there is insufficient time to obtain a warrant. Finally, under Standard 2-9.4(c)(i), if one or more of the subjects of monitoring "consents to have the tracking device accompany their person," an exception to the court order and suspicion requirements would apply.

A related issue—one that is relevant throughout the remaining standards on technologically-assisted physical surveillance—is why the cause requirements in this standard are associated with seeking evidence of crime rather than the broader criterion of performing a legitimate law enforcement function. Certainly tracking devices might be useful for reasons other than garnering evidence. For instance, they might be a means of protecting individuals from harm in situations in which no evidence of crime is sought. The standards conclude, however, that when the device is located within a private home, not every law enforcement interest is a sufficient basis to justify the surveillance. Determining when police actions might deter or prevent a crime is too speculative an inquiry where the privacy of the home will be affected. Moreover, as a practical matter, attempts to deter or prevent crime can usually be characterized as attempts to obtain evidence as well,[16] or can legitimately be accomplished through obtaining the consent of the person whom police want to protect.

Standard 2-9.5 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

16. For instance, if police have probable cause to believe someone is in imminent danger of being harmed, focusing surveillance on a private area to prevent the crime would be permissible, as it would also presumably produce evidence of crime.

(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 2-9.5(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.

Commentary to Standard 2-9.5

Standard 2-9.5 applies the same rules to both illumination devices and telescopic devices. Although they involve quite different capabilities, illumination and telescopic devices are treated together because they raise the same analytical issues, issues that in turn are different from those raised by the other types of devices treated by these standards. Unlike video surveillance and tracking devices, the devices at issue in this standard usually do not require installation in or intrusion upon property in order to be effective at surveilling private locations. They differ from detection devices in that they tend to enhance observation rather than to permit viewing of conditions that are literally unobservable from any lawful vantage point.

As with the preceding standards, Standard 2-9.5 applies a different test depending on whether the surveillance will observe a "private activity or condition." Standard 2-9.5(a) governs observation of private conduct, while Standard 2-9.5(b) governs observation in any other circumstances.

(a) Surveillance of private activity or condition

Standard 2-9.5(a) provides that use of telescopic and illumination devices to surveil "private activities and conditions" requires "probable cause to believe evidence of crime will thereby be discovered," as well as a warrant

when there are no exigent circumstances.[1] Given the definition of "private" in Standard 2-9.2(f), determining whether this probable cause requirement applies to a particular surveillance of the interior of the home and similar locations depends upon a multi-factor analysis. For example, the requirement probably would not apply to surveillance of conduct that occurs next to an uncovered window at street level, but probably would be triggered by observation of nighttime activities in a third-story bedroom from a tree on fenced-in curtilage. Brief use of a flashlight or cheap binoculars is less likely to invoke the requirement than prolonged covert reliance on a high-powered telescope or an infrared device. Other examples of this multi-factor approach abound in the cases.[2]

(b) Surveillance of other activities and conditions

Standard 2-9.5(b) governs use of illumination and telescopic devices in all circumstances "not governed by Standard 2-9.5(a)." Standard 2-9.5(b)(i) establishes that, when aimed at nonprivate areas, use of such a device that is "overt and not prolonged with respect to any given area" (*e.g.*, use of a flashlight to scan park bushes or the exterior of a house) is not subject to

---

1. Some courts have adopted an exception to the probable cause requirement when an enhancement device is used to "confirm" a suspicious naked eye sighting. *See, e.g.*, State v. Holbron, 648 P.2d 194, 197 (Haw. 1982) (finding no search where binoculars are used only to confirm unaided observations). This standard does not adopt this exception. It should also be noted, however, that in the usual confirmation situation probable cause will not be required because the activity surveilled is not "private." For instance, using binoculars to confirm that a suspected drug deal is taking place in front of a picture window in a house would probably not constitute a search for the reasons given in the text following this note.

2. *See, e.g.*, United States v. Dunn, 480 U.S. 294 (1987) (use of flashlight to view inside of barn through netting, from open fields, not a search); United States v. Lace, 669 F.2d 46, 53 (2d Cir. 1982) (continuous covert surveillance of the curtilage from private property using sophisticated equipment such as a Bushnell spotting scope with 45-power magnification, a Questar lens with 130-power magnification, infrared goggles, and a Javelin nightscope capable of magnifying existing light 50,000 times was a search); United States v. Kim, 415 F.Supp. 1252 (D.Hawaii 1976) (use of telescope to observe illegal gambling, including reading material, inside a high rise apartment is a search); Commonwealth v. Williams 431 A.2d 964 (Pa. 1981) (nine-day surveillance of a third-story apartment from another apartment using binoculars and a Startron was a search); Commonwealth v. Hernley, 263 A.2d 904 (Pa. 1970) (use of binoculars and a ladder to view through windows not a search because windows uncurtained).

regulation. In such circumstances, the insult to privacy and related interests is slight or non-existent.

On the other hand, as with long-term public video surveillance, protracted use of such devices in a conspicuous manner can be intimidating and oppressive. For instance, even though the surveillance would be overt, the effect on the public of continually scanning a public square with a large spotlight could be significant. Likewise, covert use of these devices is similar to covert video surveillance in its potential for abuse. Thus in the latter two situations, Standard 2-9.5(b)(ii) requires that the surveillance be "reasonably likely to achieve a legitimate law enforcement objective," as that phrase is defined in Standard 2-9.2(d).

In contrast to video surveillance, however, this standard does not require authorization by a supervisory officer or other official under such circumstances. The length and scope of surveillance using illumination or telescopic devices will generally not approach that of the typical video surveillance. More importantly, perhaps, the fact that these devices lack recording capacity renders them less intrusive than video cameras (recall that, under Standard 2-9.1(d)(iii), if they do have recording capacity they would be governed by the video surveillance standards).

Standard 2-9.6 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 conditions creating a lesser expectation of privacy associated with the private place;

(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;

(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 2-9.6(a) is permissible if it does not involve search of a place of residence or of a person 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 2-9.6(a)(iii), even absent any individualized suspicion of danger that otherwise would be required.

(d) Law enforcement agencies using detection devices shall 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.

Commentary to Standard 2-9.6

Standard 2-9.6 divides detection devices into three categories: general detection devices, governed by Standard 2-9.6(a); devices that detect only contraband, governed by Standard 2-9.6(b); and devices that detect only weapons, governed by Standard 2-9.6(c) (for definitions of these categories see Standard 2-9.2(b) and accompanying commentary). In addition, because of unique privacy and health and safety issues raised by the use of detection

devices, Standard 2-9.6(d) contains additional rules that should be adopted by law enforcement agencies to protect against such harms.

(a) General detection devices

Standard 2-9.6(a) deals generally with the use of detection devices "to search a private place," whether that place is associated with "a person, premises, or effect." The standard addresses such surveillance in four distinct contexts.

(i) Probable cause searches. Because general detection devices reveal more than just contraband or weapons, Standard 2-9.6(a)(i) provides that their use in connection with private activities and conditions generally requires "probable cause" (subject to certain exceptions that are set out in the rest of Standard 2-9.6(a)). This provision draws the traditional distinction between the with-warrant determination of the magistrate and the without-warrant determination of the police, depending on whether exigent circumstances are present. Standard 2-9.6(a)(i)(B)(2) also recognizes a second exception to the warrant requirement, where obtaining a warrant is "unnecessary because of conditions creating a lesser expectation of privacy associated with the private place." This provision describes those instances (usually involving search of vehicles under *California v. Carney*[1]) when Fourth Amendment law requires probable cause but no warrant because of diminished privacy expectations.

Probably the most controversial use of detection devices aimed at private places involves thermal imaging, the technique that permits law enforcement officials to identify heat sources within a building and thus facilitates location of drug laboratories or in-house marijuana farms using high-intensity lights. Because even relatively primitive thermal imaging devices can detect heat differentials as small as a half-degree (*see* commentary to Standard 2-9.2(b)), they have the potential for discerning a variety of activities associated with an expectation of privacy.

A majority of courts, however, have held that use of such a device to determine the heat output of a private place is not a search, because it merely

1. 471 U.S. 386 (1985).

detects heat "waste" that has been "abandoned" by the house occupant.[2] A few courts disagree. One court, for instance, analogized the heat waves that emanate from a heat source through the walls of a house to the sound waves picked up by a microphone.[3] In both instances, the court reasoned, it is the *source* of the waves, not the "abandoned" waves themselves, in which the police are interested. Whether thermal imaging under such circumstances is a "search" will ultimately depend, of course, upon Supreme Court resolution of the issue.

(ii) Searches not requiring individualized suspicion. Standard 2-9.6(a)(ii) addresses several situations in which the Supreme Court has permitted a search even in the absence of a belief that evidence or weapons will be found.

Standard 2-9.6(a)(ii)(A) permits suspicionless use of a detection device as to all locations that can be searched "incident to a lawful custodial arrest," because, under the Supreme Court's decisions, the police need not show probable cause or even any lesser likelihood that evidence will be found through such searches.[4] One important benefit of a detection device in this situation is that it permits the officer to avoid the immediate proximity of the arrestee, where there might be greater danger of sudden attempts to access a weapon or escape. Indeed, given this benefit, officers may want to use this type of search *before* making a custodial arrest. Under the Court's ruling in *Rawlings v. Kentucky*,[5] such a practice would not be objectionable as long as

---

2. Some of these courts also analogize thermal imaging to use of a dog to detect drugs, which the Supreme Court has indicated is not a search. United States v. Place, 462 U.S. 696 (1983). However, thermal imaging is clearly not a contraband-specific technique, and thus *Place* is not apposite here.

3. United States v. Cusumano, 67 F.2d 1497 (10th Cir. 1995), vacated on rehearing en banc, 83 F.2d 1247, on the ground that the imaging issue need not be reached because evidence from other sources provided sufficient cause for the challenged warrant.

4. *See* United States v. Robinson, 414 U.S. 218 (1973) (search of arrestee's person); Chimel v. California, 395 U.S. 752 (1969) (search of premises in arrestee's immediate proximity); New York v. Belton, 453 U.S. 454 (1981) (search of passenger compartment of car occupied by arrestee).

5. 448 U.S. 98 (1980).

the grounds for the arrest are established before use of the device and such use takes place contemporaneously with the arrest.[6]

Standard 2-9.6(a)(ii)(B) recognizes that use of a detection device is also permissible "with the consent of a person with real or apparent authority to give such consent." The Supreme Court's cases have settled that voluntary consent to a search obviates the need for any individualized suspicion.[7] Moreover, the consent option in this situation can *protect* privacy, by prompting officers to seek permission to conduct a technological search which may be less intrusive than the conduct in which they might otherwise engage (*e.g.*, rummaging through all the effects in a car).

On similar grounds, Standard 2-9.6(a)(ii)(C) allows use of a detection device directed at places the police are authorized to search "pursuant to a lawful inventory." At least in theory, detection devices can perform inventory searches in a less intrusive manner than could an officer without such a device. However, as the Supreme Court has held, inventory searches may *not* be pretextual.[8] This same rule would apply to inventory searches conducted with the use of a detection device.

(iii) Protective searches. Standard 2-9.6(a)(iii) allows the use of a general detection device when there are grounds for taking "protective action." This standard lists three such situations: frisks, "no-knock" entries, and protective sweeps of premises.

---

6. *See* 448 U.S. at 111 ("where the formal arrest followed quickly on the heels of the challenged search of petitioner's person, we do not believe it particularly important that the search preceded the arrest rather than vice versa," so long as the fruits of the search were "not necessary to support probable cause to arrest"). *See also*, Cupp v. Murphy, 412 U.S. 291 (1973) (upholding forcible removal of matter under defendant's nails prior to arrest because probable cause existed that evidence was in the process of being destroyed).

7. Schneckloth v. Bustamonte, 412 U.S. 218 (1973).

8. South Dakota v. Opperman, 428 U.S. 364 (1976). The Court's decision in Whren v. United States, 116 S.Ct. 1769 (1996) was limited to situations in which the police have probable cause and specifically exempted inventory searches, which do not require probable cause, from its holding that pretextual searches do not violate the Constitution. *Id.* at 1779.

Terry v. Ohio[9] specifies when a person detained temporarily for investigation may be frisked, while *Michigan v. Long*[10] describes those circumstances in which the person's vehicle may be examined for weapons. The justification for permitting use of general detection devices in these situations is most obvious when the device reveals characteristics rather than images (*e.g.*, the presence of metal). While an affirmative response from such a device may carry some ambiguity, its use is just as legitimate as the more traditional *Terry* pat-down, which likewise often produces the ambiguous result that there is a hard object that could be but is not necessarily a weapon.

There are also general detection devices which rely on imaging techniques, so that they reveal not only the outline of any weapon, but also the outline of other objects (perhaps to the point where they can be specifically identified).[11] Use of such a device in this context is more difficult to justify under *Terry,* which ordinarily allows a search into the clothing and removal of objects only if the pat-down reveals something which might be a weapon. However, even a pat-down reveals size, shape and density and thus also has the capacity to reveal the presence of specific objects other than weapons.

Furthermore, akin to searches incident to arrest, an "electronic frisk" may have certain advantages over the typical frisk. First, use of the device avoids the necessity for another type of highly intrusive activity, the actual placing of hands over the suspect's entire body. Second, it permits the officer to remain a safer distance from the suspect. Third, it identifies weapons with greater certainty and locates them with greater precision, so that post-frisk searches into clothing will be fewer in number and more limited in scope.

Standard 2-9.6(a)(iii)(B) similarly allows use of general detection devices when police must enter premises either to make an arrest or to execute a search warrant "without notice in the interest of self-protection." Usually police must precede entry into premises with notice of their authority and purpose.[12] However, there are exceptions to this general rule. The exception relevant here is that such notice is not required when there is reasonable

---

9. 392 U.S. 1 (1968).
10. 463 U.S. 1032 (1983).
11. *See* commentary to Standard 2-9.2(b).
12. Wilson v. Arkansas, 514 U.S. 927 (1995).

suspicion that the occupants are armed and dangerous, so that it is best for the police to take the occupants by surprise.[13]

The paradox is that the lack of notice sometimes leads to harm when those inside misperceive who is coming in and why, which is precisely why use of a detection device in this context would be especially useful. Equipment which can "see" through walls, now under development,[14] enables police to learn while still *outside* whether there is a person lurking just inside the door or a shotgun or other weapon readily accessible there. While such use of the device does constitute a Fourth Amendment search, it is a justifiable search, for it permits the police to see what they would otherwise discover if they instead made the traditional entry without notice. An added benefit of such searches would be that they would on some occasions dissipate the fear of danger, so that bypassing notice before actual entry would then become unnecessary.

Standard 2-9.6(a)(iii)(C) allows use of a detection device to search places the police are authorized to "subject to a protective sweep." This refers to the holding in *Maryland v. Buie*,[15] in which the Court adopted a two-pronged test regarding the reasonableness of a protective sweep to protect officers who are lawfully within premises to make an arrest. Specifically, the police may (1) enter "spaces immediately adjoining the place of arrest from which an attack could be immediately launched," and (2) may enter more remote parts of the premises on a reasonable suspicion that the area "harbors an individual posing a danger to those on the arrest scene."[16] Consistent with *Buie*, this standard permits police to use a detection device capable of looking through walls and similar barriers to make essentially the same search under the same circumstances and on the same grounds. Conducting the protective sweep in this fashion has several advantages: it would be in some respects less intrusive; it would tend to give the officer a more definite reading concerning others on the premises; and it would avoid the danger of a surprise confrontation.

---

13. *Id.*
14. *See* commentary to Standard 2-9.2(b).
15. 494 U.S. 325 (1990).
16. 494 U.S. at 334.

It must be emphasized that, in all of these situations, a general detection device, by definition, might reveal other items in addition to weapons. For example, in a *Buie* scenario, use of such a device to determine whether confederates are lurking in a closet might reveal objects in locations in which a person would never be sought or found (*e.g.*, a small container). The assumption of this standard is that the device normally will disclose only what police officers would be able to feel (through a frisk) or see (through a search) if they acted to the full extent of their authority. To the extent the device allows police to go beyond that authority, the general principles set out in Standard 2-9.1(c)(iv) (which requires consideration of whether a technique "is less intrusive than other available effective and efficient alternatives") and Standard 2-9.1(d)(ii) (which requires that the scope of surveillance "be limited to its authorized objectives and be terminated when those objectives are achieved") may dictate that the technique should not be used.

(iv) Checkpoints. Standard 2-9.6(a)(iv) addresses the situations in which detection devices may be used in connection with "persons or effects passing a checkpoint." There are three types of checkpoints discussed in this section: a fixed checkpoint designed to find contraband; a fixed checkpoint designed to find weapons; and a temporary checkpoint to prevent serious bodily harm.

Because all three of these situations involve seizures and searches of groups of people, involvement of upper level officials is essential. Thus, Standard 2-9.6(a)(iv) requires that the first two types of checkpoints be authorized by "an appropriate politically accountable law enforcement official or governmental authority" and that the third type of checkpoint be approved by a "supervisory law enforcement official" (the latter difference reflecting the relatively urgent nature of such checkpoints).

The standard also provides for public involvement in connection with the two types of fixed checkpoints, of the same kind required in connection with long-term overt use of video surveillance (*see* Standard 2-9.3(b)(ii)). Such long-term checkpoints can have a major impact on the community in which they are located. For this reason, the community should have some means of providing input as to its necessity, duration, and implementation.

One other limitation, which is imposed on all three types of checkpoints, is especially important to note. Consistent with the general principle in

Standard 2-9.1(d)(i), those subjected to detection device checkpoints must be selected in a fair and consistent manner. In this context, this principle will generally mean that police must aim the detection device at all of those who arrive at the checkpoint, or at least at all who are selected on some pre-arranged non-discriminatory basis (*e.g.*, every fifth person). Choosing whom to subject to the device at the time of their arrival is a procedure prone to abuse.

As noted, Standard 2-9.6(a)(iv)(A) deals with the contraband checkpoint. The provision that the checkpoint serve a "compelling government interest that no contraband pass by" is meant to embody a requirement that the checkpoint be an effective way of achieving a government aim of the greatest magnitude.[17] This high standard is necessary when searches are undertaken on a group rather than individualized basis. Indeed, perhaps the only situation in which this test is met is where entry into an area may be conditioned upon passersby establishing they do not have contraband with them.

Standard 2-9.6(a)(iv)(B), dealing with weapons checkpoints, likewise requires proof of a "compelling government interest," this time defined as an interest in ensuring "that no weapons pass by that checkpoint into a place where the presence of weapons would be extraordinarily hazardous." This standard is consistent with existing Fourth Amendment law in permitting checkpoints in environments where introduction of a weapon would be so uniquely hazardous that the government has a valid interest in ensuring all who enter are unarmed. The classic illustration is the airport hijacker detection system, which is grounded in the understandable notion that the potential hijacker must be dealt with before he or she boards an airplane with a weapon. Other situations that fall within this general category include checkpoints for visitors at prisons and certain public buildings such as courthouses where the need for deterrence and protection is extremely strong.

If a weapon-specific device were available, one might require that this latter type of checkpoint use it, in light of the general principle in Standard 2-9.1(d)(iv) encouraging the least restrictive alternative. However,

---

17. *Compare* Michigan State Police v. Sitz, 496 U.S. 444 (1990) (requiring only that the government demonstrate that a sobriety checkpoint is a reasonable way of deterring or detecting drunk drivers).

authorizing use of general detection devices in such situations is not inconsistent with existing law, which permits x-ray and magnetometer searches that are not limited to discovery of a weapon.[18] Given the risk sought to be averted, this added intrusion is justifiable.

Standard 2-9.6(a)(iv)(C) deals with the occasional situation in which a strong interest in preventing death or serious injury is compelling enough to justify a one-shot use of a detection device against a group of persons, effects, or places. It permits the use of detection devices at a checkpoint which is "temporary and has been established in response to a substantial risk of death or serious bodily harm." This checkpoint is not only not founded on individualized suspicion, but is also not confined, like the fixed checkpoints are, to an area that by its nature is associated with compelling governmental needs (*e.g.*, prisons, borders, or airports). Therefore, special diligence in ensuring the group is not selected on some discriminatory basis is necessary. Consequently the standard takes the position that such preventive measures must be based on "reasonable suspicion" that by using the detection device against the anticipated group of persons, effects or places, the weapon or person endangered "would thereby be discovered." In addition, the "anticipated size of the group of persons involved" must be "reasonable" in light of the problem to which this preventive measure is being applied.

Under this standard, the detection device sometimes will be used to locate the item which is the source of the danger. An illustration would be the situation in which authorities receive a tip that a bomb has been placed within an unidentified piece of luggage for a particular train. The tip would provide a basis for screening all the checked luggage for that train.

Alternatively, the device might be used to find the endangered person or persons, as where an area in which a kidnapping recently occurred is cordoned off so that all vehicles leaving the area can be checked for the kidnap victim. This latter illustration recalls Justice Jackson's oft-quoted observation in *Brinegar v. United States*[19] that he would "candidly strive hard" to uphold a roadblock in such circumstances, even though the police were to "search every outgoing car," as "it might be reasonable to subject

---

18. *See, e.g.*, United States v. Montoya de Hernandez, 473 U.S. 531 (1985) (use of x-ray to find drugs).

19. 338 U.S. 160 (1949).

travelers to that indignity if it was the only way to save a threatened life."[20] The case for allowing such a procedure is considerably stronger where, as contemplated under this provision, the vehicles are only subjected to a detection device which could reveal the kidnap victim without the necessity of any physical search.

A final issue in connection with detection device checkpoints concerns pre-surveillance notice. Both Standard 2-9.1(d)(v) and existing Fourth Amendment law[21] recognize, when deterrence is the goal, the importance of announcing in some way the nature of the checkpoint and the detection devices in place there (*e.g.*, by posting a sign or making a statement on a public address system). As one court has said, "Advance notice enables the individual to avoid the embarrassment and psychological dislocation that a surprise search causes."[22] Of course, when the checkpoint is of the third type (*e.g.*, designed to apprehend a kidnapper), a warning would sometimes defeat the law enforcement objective and should not be required. Even in this situation, however, once stopped, those subjected to the checkpoint are entitled to some explanation for the stop.

When pre-surveillance notice is required, the courts have also extended to potential checkpoint subjects "the right to leave rather than submit to the search."[23] The basic point of these decisions is that this special search power, grounded as it is in unique problems existing at a particular place, cannot rationally be exercised over those who elect not to go to that place. If there is a right to leave the site of the checkpoint, it follows that the act of leaving does not itself bring into play a right to search, although such a decision, together with other circumstances, might on occasion constitute a reasonable suspicion justifying protective search activity.

(b) Contraband-specific devices

Standard 2-9.6(b) concerns the use of a "contraband-specific device to search a private place" other than in the circumstances authorized under Standard 2-9.6(a). Because such devices, by definition, detect only drugs,

---

20. 338 U.S. at 183 (Jackson, J., dissenting).
21. *See, e.g.*, United States v. Davis, 482 F.2d 893 (9th Cir. 1973).
22. People v. Hyde, 525 P.2d 830 (Cal. 1974) (Wright, C.J. concurring).
23. United States v. Davis, 482 F.2d 893 (9th Cir. 1973).

weapons and other items that are illegally possessed,[24] they may be used in situations in which general detection devices may not be. This position is based on two Supreme Court cases. In *United States v. Place,*[25] the Supreme Court indicated that a dog sniff of luggage to determine if it contained drugs was not a search. The primary rationale for this holding was the unintrusive nature of a dog sniff; the dog does not invade the contents of the suitcase and only alerts to items inside the luggage that are illegal contraband. In *Jacobsen v. United States,*[26] the Court engaged in similar analysis in holding that when a substance has come into police control without a violation of the Fourth Amendment, a drug test of that substance establishing that it is cocaine invades nothing of "privacy significance" and thus does not implicate the Fourth Amendment. From these two cases the conclusion can be drawn that, if a police action does not involve a physical intrusion and discovers only contraband, it is not a Fourth Amendment search regardless of where the contraband is located.

Nonetheless, Standard 2-9.6(b) places some limits on the use of contraband-specific devices. First, such devices may not be used to conduct a "search of a place of residence or of a person" unless probable cause or one of the exceptions outlined in Standard 2-9.6(a) exist. This provision is meant to provide an ultimate place of repose (i.e., the citizen's home and body) that is sacrosanct from suspicionless government intrusion, even when that intrusion is only designed to discover the presence of contraband, does not harm its target, and is used covertly (thus avoiding any direct atmosphere of oppression).

Standard 2-9.6(b) also imposes limits on the use of contraband-specific devices aimed at locations other than a home interior or a person. First, it requires that such use be "reasonably likely to achieve a legitimate government enforcement objective." Second, where a seizure is necessary

---

24. Recall from the definition in Standard 2-9.2(b) that whether a device is contraband-specific depends not only on whether it reveals only the presence of contraband, but also on the circumstances of its use. Thus, for instance, while a weapons-detector in an airport would be a contraband specific device, the same detector used in the streets of a jurisdiction which permits concealed weapons would not be.

25. 462 U.S. 696 (1983).

26. 466 U.S. 109 (1984).

to use the device, there must also be "grounds for the seizure." Thus if a full stop of the person is necessary to use the device, reasonable suspicion is required.[27] Even if no seizure is involved, aiming a detection device at people is likely to be disconcerting, if not alarming. This standard thus takes the position that police may not randomly aim a detection device at any passerby from their police cruiser or as they walk down the street. Such non-seizure surveillance should only be permitted when designed to discover evidence of a particular crime or type of crime (such as using a drug-detection device in the vicinity of an open-air drug market), or to prevent serious physical harm to others.

(c) Weapon-specific devices

Standard 2-9.6(c) addresses the use of "weapon-specific detection devices." In many situations (*e.g.*, airports, jurisdictions where carrying a concealed weapon is a crime), a weapon-specific device will also be a contraband-specific device. However, in those jurisdictions in which carrying a concealed weapon is not a crime, use of such a device would be a search, because it would not be authorized by the *Place-Jacobsen* rationale. Nonetheless, Standard 2-9.6(c), through its cross-reference to Standard 2-9.6(a)(iii)(which deals with use of general detection devices for protective purposes), permits use of a weapon-specific device even in the latter jurisdictions whenever police have lawfully stopped an individual, as well as when they can lawfully enter premises without notice or conduct a protective sweep.

It was explained earlier why use of a general detection device to frisk must be preceded by grounds both for the stop and the frisk. This provision, however, specifically eliminates any requirement that suspicion of danger, typically required for a frisk, exists. When the search is narrowed to what a weapon-specific device would detect, it should be permissible even when a reasonable officer would not have harbored a suspicion that the person was armed and dangerous, for the only intrusion into privacy has been to identify that in fact there *was* potential danger.

---

27. *Place* makes it clear that, notwithstanding the non-search character of a dog sniff, a seizure of persons or effects made to facilitate such non-search activity is Fourth Amendment activity subject to the usual individualized suspicion requirement. 462 U.S. at 707-10.

For the same reason, this provision permits, without any articulable suspicion of danger, use of a weapon-specific device to surveil inside an entrance prior to a home entry authorized on probable cause, as well as the vicinity of an arrest subsequent to the arrest taking place. Again, the theory is not that the device only permits discovery of contraband (for in many states weapons may not fit that definition). Rather it is that in contexts where protective action would be authorized based on individualized suspicion, a device which detects only weapons can be used even absent that suspicion because all it does is ensure that the protection occurs.

As a practical matter this provision does not add much to police power. As noted earlier, courts have long recognized that the requisite "armed and dangerous" probability for a frisk is lower than the probability of criminality needed for the stop itself. This is as it should be, for the tolerable risk that otherwise an officer might be shot is well below the tolerable risk that some criminal offense might continue undetected. With the proliferation of weapons in recent years, courts have broadened even more the circumstances in which a protective frisk is appropriate,[28] to the point where it is almost coincident with the automatic "frisk" authority discussed here.

(d) Restrictions on use

Standard 2-9.6(d) calls upon law enforcement agencies using detection devices to adopt procedures to ensure that certain dangers specific to detection devices will be avoided. To the extent detection devices have been developed which have the virtual capacity to "electronically strip" passersby, Standard 2-9.6(d)(i) would limit the exposure of information which involves the "disclosure of gender-specific anatomical features to officers of the opposite gender." Standard 2-9.6(d)(ii) cautions police against inappropriate use of "active" devices that may, through x-ray or some other technology, cause physical harm to the target.

---

28. *See* David Harris, *Frisking Every Suspect: The Withering of Terry*, 28 U.C. DAVIS L. REV. 1, 5 (1994) (concluding, based on trends in the case law, that "[s]oon *anyone* stopped by police may have to undergo a physical search at the officer's discretion, however benign the circumstances of the encounter or the conduct of the 'suspect'").