Copyright © 2001 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 review or for non-profit educational and training use provided proper attribution is given to the American Bar Association.

Library of Congress Catalog Card No. 2001134054
ISBN-1-59031-050-0

The commentary contained herein does not necessarily represent the official position of the American Bar Association. 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, N.W.
Washington, D.C. 20005
202/662-1500

Printed in the United States of America
ABA Standards for Criminal Justice
Electronic Surveillance
Third Edition
Section A: Electronic Surveillance of Private Communications

ABA Section of Criminal Justice
Ronald C. Smith, Chair, 2001–2002
Ralph C. Martin II, Chair, 2000–2001
Bruce M. Lyons, Chair, 1999–2000
Myrna Raeder, Chair, 1998–1999
Ronald Goldstock, Chair, 1997–1998

Criminal Justice Standards Committee
Ronald Goldstock, Chair, 2000–2002
Niki Kuckes, Chair, 1998–2000
Charles R. English, Chair, 1997–1998

Task Force on Technology and Law Enforcement
Sheldon Krantz, Chair
Martin Marcus, Reporter

Standards approved by ABA House of Delegates
February 2001

Commentary completed
November 2001
ABA Criminal Justice Standards Committee

Chair and Members

Ronald Goldstock, Chair
Independent Private Sector Inspector General,
Larchmont, New York

Steven H. Goldblatt
Professor, Georgetown University Law Center, Washington, D.C.

Mathias Henry Heck, Jr.
Montgomery County Attorney, Dayton, Ohio

Sterling Johnson, Jr.
Judge, U.S. District Court, Eastern District of New York
Brooklyn, New York

Albert J. Krieger
Private practitioner, Miami, Florida

Rory Little
Professor, Hastings College of Law, University of California,
San Francisco, California

Martin Marcus
Judge, New York State Supreme Court, Bronx County, New York

Irma S. Raker
Judge, Maryland Court of Appeals, Rockville, Maryland

Charles Z. Smith
Justice, Washington State Supreme Court, Olympia, Washington

November 2001
Liaisons to the Standards Committee

Herbert B. Dixon  
ABA Judicial Division

Matthew Mertens  
U.S. Department of Justice

Robert E. Shepherd, Jr.  
ABA Juvenile Justice Center

William A. Helm  
National Association of Attorneys General

Peter Goldberger  
National Assn. of Criminal Defense Lawyers

Norman K. Maleng  
National District Attorneys Association

Scott Wallace  
National Legal Aid & Defender Association

November 2001

Standards Committee Staff

Susan W. Hillenbrand

During the preparation of the Standards on Electronic Surveillance of Private Communications, the Standards Committee was also chaired by Charles R. English, Santa Monica, California (1997-1998) and by Niki Kuckes, Washington, D.C. (1998-2000). The following also served on the Criminal Justice Standards Committee during the preparation of these Standards: Justice Michael L. Bender, Denver, Colorado; Judge Johanna L. Fitzpatrick, Alexandria, Virginia; Justice Henry E. Frye, Raleigh, North Carolina; Mary Frances Harkenrider, Chicago, Illinois; Robert M. A. Johnson, Anoka, Minnesota; David A. Reiser, Washington, D.C.; Professor Stephen A. Saltzburg, Washington, D.C.; Professor Karen R. Smith, Los Angeles, California; Judge Thomas Smith, Jr., Mount Holly, New Jersey; and Jo-Ann Wallace, Washington, D.C. Kathleen A. Felton and Steven Bunnell also served as liaisons from the U.S. Department of Justice.
Task Force:  
Technology and Law Enforcement

Chair and Members

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

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

Reporter

Martin Marcus
Judge, New York State Supreme Court, Bronx County, New York
Liaisons to the 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

David Larson
Federal Bureau of Investigation

Eric M. Noonan
National Association of Attorneys General

Terrence Sheridan
Major Cities Chiefs

Jo-Ann Wallace
National Legal Aid and Defender Association

Kevin L. Wright
National District Attorneys Association

Task Force Associate

Mark Eckenwiler
U.S. Department of Justice

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.
| Standard 2-4.1 | Order authorizing electronic surveillance; authorized application | 91 |
| Standard 2-4.2 | Application; form; contents; additional facts | 95 |
| Standard 2-4.3 | Probable cause; kinds of showings | 103 |
| Standard 2-4.4 | Designated offenses; criteria | 109 |
| Standard 2-4.5 | Other offenses | 112 |
| Standard 2-4.6 | Judicial discretion and determination | 117 |
| Standard 2-4.7 | Order; jurisdiction | 119 |
| Standard 2-4.8 | Order; form; contents | 123 |
| Standard 2-4.9 | Minimization after communications intercepted | 135 |
| Standard 2-4.10 | Order not specifying place or facilities; application and authorization | 144 |
| Standard 2-4.11 | Extensions | 147 |
| Standard 2-4.12 | Privileged communications | 149 |
| Standard 2-4.13 | Orders and applications; custody; destruction | 150 |
| Standard 2-4.14 | Authenticity | 150 |
| Standard 2-4.15 | Inventory; contents; time; postponement | 159 |
| Standard 2-4.16 | Disclosure; use | 161 |
| Standard 2-4.17 | Reports | 164 |

**PART V. INTERCEPTION OF COMMUNICATIONS BY LAW ENFORCEMENT WITHOUT AN ELECTRONIC SURVEILLANCE ORDER**

| Standard 2-5.1 | Intercepting communications with consent | 167 |
| Standard 2-5.2 | Intercepting communications in an emergency situation | 171 |

**PART VI. SANCTIONS**

| Standard 2-6.1 | Sanctions, in general | 179 |
| Standard 2-6.2 | Evidentiary sanctions; exceptions | 179 |
| Standard 2-6.3 | Criminal sanctions | 192 |
| Standard 2-6.4 | Civil sanctions | 193 |

**PART VII. ADMINISTRATIVE REGULATIONS**

| Standard 2-7.1 | Administrative regulations | 195 |
PART VIII. PRIVATE COMMUNICATIONS ACQUIRED BY AND RECEIVED FROM ELECTRONIC COMMUNICATION SERVICE PROVIDERS

Standard 2-8.1 Communications acquired by an electronic communication service provider 197
Standard 2-8.2 Communications received by law enforcement from an electronic communication service provider 204
Standard 2-8.3 Communications received by other persons from an electronic communication service provider 211
INTRODUCTION

The History of the Standards

In 1968, shortly before the enactment of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, the Advisory Committee on the Police Function published the Tentative Draft of Standards Relating to Electronic Surveillance. The Draft Standards were substantially similar, but not identical, to the provisions of Title III.¹ In the process by which the Draft Standards were considered and approved by the Special Committee on Standards for the Administration of Criminal Justice, the Criminal Law Council, and the ABA House of Delegates, the Standards were amended to bring them even closer to Title III.² In its final form, the First Edition of the Standards Relating to Electronic Surveillance was approved by the ABA House of Delegates in February of 1971.

¹ The similarity is not entirely surprising, since the principal author of Title III, G. Robert Blakey, served both as Counsel to the U.S. Senate Judiciary Committee at the time Title III was drafted and enacted, and as the Reporter for the Advisory Committee on the Police Function.

² See ABA Project on Standards for Criminal Justice, Standards Relating to Electronic Surveillance (Approved Draft, 1971) [hereinafter “the First Edition”], General Commentary at 1. For example, reflecting the language of Title III limiting who may authorize an application for an electronic surveillance order, Standard 1.1 was amended to restrict applicants for court authorized electronic surveillance to “the Attorney General of the United States, or the principal prosecuting attorney of a state or local government, or law enforcement attorneys or officers acting under his direction.” Similarly, Standard 5.3, which concerns the contents of an application for an electronic surveillance order, was amended to add the requirements of Title III that such an application contain the identity of the law enforcement officer making the application and (as the Supreme Court said was necessary in Berger v. New York, 388 U.S. 41 [1967]) a particular description of the type of communications sought to intercepted. Concerning amendments proposed by the Criminal Law Council which the House of Delegates rejected, see First Edition, General Commentary at 2-4.
Introduction

Since 1968, prosecutors have made extensive use of Title III, and the courts, including the Supreme Court, have been called upon repeatedly to interpret its provisions. The judicial interpretations of Title III have themselves been subjected to extensive scholarly commentary. In 1978, a second edition of the Standards was approved, in which the Standards and commentary were amended to reflect some of these judicial and scholarly developments, but “the second edition of the standards continue[d] to resemble Title III in large measure.” The commentary was amended again in 1986, but the Standards were not.

3. In 1967, the Supreme Court issued two decisions which enabled Congress to draft an electronic surveillance statute that satisfied the requirements of the Fourth Amendment: Katz v. United States, 389 U.S. 347 (1967) (declaring electronic surveillance a search and seizure requiring a court order supported by a showing of probable cause); and Berger v. New York, 388 U.S. 41 (1967) (setting forth the constitutional requirements for court ordered electronic surveillance). Since Title III was enacted, the Court has considered issues relating to the interception of wire or oral communications many times. See United States v. Alderman, 394 U.S. 165 (1969) (concerning standing to move to suppress intercepted communications); Gelbard v. United States, 408 U.S. 41 (1972) (concerning right of grand jury witness who refuses to answer questions to assert as defense to civil contempt charge claim that questions asked were derived from illegal electronic surveillance); United States v. Giordano, 416 U.S. 505 (1974) (concerning who may authorize an application for an electronic surveillance order under Title III); United States v. Chavez, 416 U.S. 562 (1974) (concerning the requirement that the official who authorized an application for an electronic surveillance order be named in the application); United States v. Kahn, 415 U.S. 143 (1974) (concerning authorization to intercept communications of parties not named in an electronic surveillance order, and the obligation to identify in the application those persons who will be subject to electronic surveillance); United States v. Donovan, 429 U.S. 413 (1977) (concerning obligation to identify in the application for an electronic surveillance order those persons who will be subject to the surveillance, and the obligation to give notice, after the surveillance, to those persons whose conversations were intercepted); United States v. Scott, 436 U.S. 128 (1978) (concerning obligation to minimize the interception of non-pertinent and privileged communications); Dalia v. United States, 441 U.S. 238 (1979) (concerning authority of law enforcement to enter premises covertly to install electronic surveillance device); United States v. Ojeda Rios, 495 U.S. 257 (1989) (concerning the obligation to seal immediately the recordings of intercepted communications); Bartnicki v. Vopper, 532 U.S. 514 (2001) (concerning First Amendment right of media companies to broadcast illegally intercepted telephone conversation when conversation was of public importance and companies had played no part in its illegal interception).


Introduction

Like the original provisions of Title III, the First and Second Editions of the Standards were applicable only to the interception of wire and oral communications. In 1986, shortly after the Commentary was last revisited, Congress enacted the Electronic Communications Privacy Act (hereinafter "ECPA"). In ECPA, Congress recognized the obvious: that the non-consensual interception of electronic communications is governed by the Fourth Amendment, and thus must meet the constitutional requirements for search and seizure. Beyond these requirements, Congress also extended to the interception of electronic communications many, but not all, of the same non-constitutional, statutory protections it gave in Title III to wire and oral communications. Finally, Congress also amended Title III to permit "roving" electronic surveillance.

In the ensuing fifteen years, many significant changes have occurred. New forms of electronic communication have developed, and the technology of both telephonic and electronic communications has changed drastically. Perhaps most significantly, the extent to which business and the general public use electronic communication and new forms of telephonic communication has exploded. At the same time, law enforcement experience with the interception of electronic communications has grown, and the courts and commentators have begun exploring the ways in which Title III, even as amended by ECPA, has been outstripped by these developments.

Beginning in 1997, the Task Force on Technology and Law Enforcement took up its assignment to prepare the Third Edition of the Standards on Electronic Surveillance. Specifically, the Task Force considered whether experience with and the interpretation of Title III suggested the need for additions to or changes in the Standards; how to modify the Standards in light of the changes made to Title III by ECPA; whether technical advancements in wire and oral communications required changes in the Standards; and how the interception of electronic communications and the access to stored electronic communications should

---


8. Concerning such surveillance, see Standard 2-4.10 and its commentary.

Introduction

be regulated. On November 20, 1999, after two and a half years of work, the Task Force presented its proposed Standards to the Committee on Criminal Justice Standards. On April 1, 2000, after revision, the Standards Committee approved and presented the proposed Standards to the Criminal Justice Council. After further revision, the Criminal Justice Council approved the Standards on July 9, 2000. At its mid-winter meeting in February of 2001, thirty years after it approved the First Edition of the Standards on Electronic Surveillance, the House of Delegates approved this, the Third Edition of the Standards.

The Themes of the Standards

These new Standards are a product of three years of effort by experts in the field of criminal procedure in general, and electronic surveillance in particular. They also reflect an attempt to establish, in a field revolutionized by ever more complex and intrusive technology, the delicate balance between the privacy rights of individuals, on the one hand, and the legitimate needs of law enforcement and the legitimate rights of communication service providers, on the other. Underlying the revision of the Standards are a variety of interrelated themes. First, electronic surveillance should continue to be regulated by standards more demanding than those applicable to other forms of search and seizure.\(^\text{10}\) Second, electronic surveillance should be governed by a single set of standards, regardless of the form of private communications subject to surveillance. Third, standards governing electronic surveillance must not merely reflect current communications and surveillance technology, but must anticipate—indeed, should strive to break free from the constraints of—developing technology. Fourth, electronic surveillance standards should emphasize the need for close supervision of those who execute electronic surveillance orders and accountability for those who apply for such orders and oversee their execution. Fifth, electronic surveillance standards should provide protection for private communications that are electronically stored, and should address the rights and responsibilities of those who provide electronic communication services. Finally, standards governing electronic surveillance should recognize that technol-

\(^{10}\) There is one exception. Standard 2-9.3(a) of the Standards on Technologically-Assisted Physical Surveillance provides that video surveillance of a private activity or condition should be governed by the same standards applicable to electronic surveillance. Concerning the overlap between the two in the context of establishing the necessity of video or aural surveillance, see the commentary to Standard 2-4.3(c).
ogy is a double-edged sword, which, depending upon how it is wielded, can undermine or enhance important privacy interests, legitimate law enforcement needs, and the rights of those who are investigated and prosecuted by the use of electronic surveillance.

The Scope of the Standards

While the Third Edition of the Standards Relating to Electronic Surveillance represents an attempt to cover the subject of electronic surveillance comprehensively, there are a few areas it does not address. First, it abandons the minimal attempt made in the First and Second Edition of the Standards to regulate electronic surveillance relating to foreign intelligence activities. Standard 2-3.1 of the Second Edition (like its counterpart in the First) stated generally that "appropriate federal officers" should be permitted to use electronic surveillance "to protect the nation from attack by or other hostile acts of a foreign power or to protect military or other national security information against foreign intelligence activities," but that such surveillance should be "subject to appropriate presidential and congressional standards and supervision." The Criminal Justice Council, however, received comments expressing grave concern about retaining this Standard, even in a modified form, since the list of purposes for which it authorized electronic surveillance is more limited than the purposes for which the Foreign Intelligence Surveillance Act ("FISA") does so. Determining whether

11. Standard 2-3.2 of the Second Edition of the Standards provides for the use and disclosure of communications obtained by such electronic surveillance, but again without significantly attempting to regulate the process. That Standard simply says that such communications may be received in evidence only "where the overhearing or recording was reasonable," and that other use of such communications should be "limited to the use or disclosure necessary to achieve the purpose of the overhearing or recording or on a showing of good cause before a judicial officer."

12. See 50 U.S.C. §§ 1801-1811. For example, FISA authorizes warrantless electronic surveillance in certain circumstances, see 50 U.S.C. § 1802, and court-ordered electronic surveillance in others, see 50 U.S.C. § 1804, and in both circumstances limits the surveillance to the acquisition of "foreign intelligence information." For purposes of both the warrantless and court-ordered surveillance, 50 U.S.C. § 1801 defines "foreign intelligence information" as: "(1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against—(A) actual or potential attack or other grave hostile acts of a foreign power; (B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
the authorized purposes for foreign intelligence surveillance should be expanded to make them consistent with federal law was a matter beyond the expertise of the Task Force, and considering that question and whether the ABA should make more specific recommendations about how the President and Congress should sets standards for and supervise foreign intelligence surveillance is more properly the subject of a separate inquiry. Thus, the Third Edition of the Standards makes no reference to foreign intelligence surveillance.

Second, the Task Force decided that even though the revised Standards govern the interception of the contents of private communications, they should not address the capture of transactional data relating to such communications. Thus, as in its previous editions, the Standards do not consider under what circumstances law enforcement should be permitted to use pen register or trap and trace devices. Similarly, they do not consider when law enforcement should have access to the routing information that directs and accompanies electronic mail as it is transmitted from the sender to the recipient. The Task Force decided not to consider these subjects, not because they were unworthy of consideration, but rather because access to such transactional data raises issues more appropriately the subject for a separate set of standards that make comprehensive recommendations for "transactional surveillance." Such standards could consider not only access to transactional data relating to communications, but other types of real-time transactional surveillance

(2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to—(A) the national defense or the security of the United States; or (B) the conduct of the foreign affairs of the United States.”

13. The Introduction to the Second Edition of the Standards, at 2.5, explained that the decision not to add standards governing the use of pen registers and similar devices “was based, in part, on the recent decision of the United State Supreme Court in United States v. New York Telephone Company [434 U.S. 159 (1977)] holding that, although pen registers are not governed by Title III, a federal judge has power under Rule 41 of the Federal Rules of Criminal Procedure to authorize the installation of such a device.” Thereafter, in Smith v. Maryland, 442 U.S. 735 (1979), the Supreme Court held that the use of a pen register was not a search within the protection of the Fourth Amendment and thus did not require the issuance of a search warrant based on probable cause. In 1986, when ECPA was enacted, Congress added rules governing the use of pen registers and trap and trace devices, requiring a court order based upon an application from “[a]n attorney for the Government” which contains “a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by [a law enforcement] agency.” 18 U.S.C. § 3121, et seq. Concerning state statutory provisions, some of which follow federal law, and some of which are more demanding, see 1 Carr, The Law of Electronic Surveillance (2000), at 4-160 - 4-161.
Introduction

as well, for example, real-time surveillance of the movement of a cell phone or of a car traveling along an electronic toll road. Because the issues are closely related, such standards could also consider the appropriate rules for access to and disclosure of historical transactional records (e.g., credit card records, frequent flier program records, or photographs of vehicles leaving airports).

A third subject not addressed by the revised Standards is encryption. Standard 2-3.1(b) announces that "law enforcement agencies should, in appropriate cases and under appropriate regulation, have the legal authority and the technological means to conduct electronic surveillance." Because powerful programs for encrypting communications are now readily available on the general market, the question arises whether, when law enforcement receives judicial authority to intercept communications that are encrypted, that authority should include the power to demand from the communications provider the technical means to decrypt the communications. Proponents for such authority fear that without it, the legitimate, court-authorized goals of a law enforcement investigation can be easily thwarted. The opponents argue that encryption has become a powerful tool for privacy at a time when communications are increasingly vulnerable to illegal interception. Despite extended discussion, no consensus emerged within the Task Force on this issue, which will continue to evolve with further developments in the technology of encryption and decryption and with further consideration in Congress and elsewhere. 14

Finally, the Standards do not directly address the changes made in Title III and the Electronic Communications Privacy Act by the USA PATRIOT

14. In the absence of legal authority for requiring an electronic communication service provider to provide a law enforcement officer with an encryption key when a court orders that encrypted communications may be intercepted, law enforcement continues its search for other means to decrypt communications. Inevitably, some of those means will be subject to legal challenge. See “F.B.I. Use of New Technology to Gather Evidence Challenged,” New York Times, July 30, 2001, p. C7, describing a challenge by defendant Nicodemo S. Scarfo, Jr., to “evidence gathered by a controversial new law enforcement technology: a system that recorded every keystroke typed on a computer, including the password that investigators used to unscramble Mr. Scarfo’s files.” The defendant claims, inter alia, that the use of this “key logger” system required an electronic surveillance order. Invoking the Classified Information Procedure Act, the Justice Department has resisted publicly revealing how the system works. “U.S. Refuses to Disclose PC Tracking,” New York Times, August 25, 2001, p. C1. Instead, the Department filed papers with the court offering to provide the defendant with an “unclassified summary statement,” and the judge with “a more complete description.” Id., p. C2.
Act,\textsuperscript{15} the anti-terrorism law enacted in response to the destruction of the World Trade Center and the attack on the Pentagon on September 11, 2001. Because the Act became law after the Standards were adopted by the House of Delegates, the Task Force and Standards Committee could not consider its provisions in drafting the Standards.\textsuperscript{16} Those provisions of the Act that modify Title III and ECPA are, however, noted in the commentary;\textsuperscript{17} those that amend the Foreign Intelligence Surveillance Act are not. It is important to note, however, that while a FISA order could previously issue only when an appropriate Federal official applying for the order certified, inter alia, "that the purpose of the surveillance is to obtain foreign intelligence information," 50 U.S.C. § 1804(7)(B) [emphasis supplied], the official now need certify only that it is "a significant purpose." USA PATRIOT Act, § 218. As a result of this change, court-ordered FISA surveillance is permissible when it is undertaken both for purposes of gathering foreign intelligence information and for use in a criminal prosecution, so long as the former purpose is "a significant" one.

This change is less dramatic than might appear from simply comparing the language of the statute before and after its amendment, since a number of courts have interpreted the requirement that "the purpose" of the surveillance be to obtain foreign intelligence information to mean that it be "the primary purpose" of the surveillance, thus permitting a FISA order to be obtained even when a criminal prosecution was a purpose, but not the primary one, of the surveillance.\textsuperscript{18} Nonetheless, in commenting on this aspect of the USA PATRIOT Act before it was enacted, the American Bar Association's Task Force on Terrorism and the Law

\textsuperscript{15} The full name of the Act, which was signed into law by President Bush on October 26, 2001, is the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001.

\textsuperscript{16} The Act, however, makes at least one change recommended by the Standards—that the acquisition of a stored wire communication be treated the same as the acquisition of a stored electronic communication, and no longer be subject to the more stringent requirements applicable to the interception of a wire communication while still in transmission. See the commentary to Standard 2-2.1(a)(ii).

\textsuperscript{17} See the commentary to Standards 2-2.1(a), 2-2.1(c)(ii); 2-4.16; 2-5.2(b); 2-8.1(a); 2-8.1(b)(i); 2-8.1(b)(iii)(B); and 2-8.2(a)(ii) and (iii).

\textsuperscript{18} See, e.g., United States v. Johnson, 952 F.2d 565, 572 (1st Cir. 1991); United States v. Pelton, 835 F.2d 1067, 1075-76 (4th Cir. 1987). See also United States v. Duggan, 743 F.2d 59, 77 (2d Cir. 1984) (requiring that obtaining foreign intelligence information be "the primary objective of the surveillance"); United States v. Truong Dinh Hung, 629 F.2d 908, 915 (4th Cir. 1980) (approving warrantless electronic surveillance before the enactment of FISA when conducted "'primarily' for foreign intelligence reasons").
Introduction

expressed its "concern that changing the standard for FISA collection so that it can be used with a clear understanding that there is a law enforcement aspect as well as an intelligence aspect may tend to reduce the protections now available under Title III and blurs the current distinction between criminal investigations and foreign intelligence surveillance."¹⁹

The new Standards also include many stylistic changes, intended to make them more comprehensible, rather than to alter their meaning or intent. Thus, for example, because Standard 2-2.1 defines the term "electronic surveillance," that term replaces the words "the use of electronic surveillance techniques . . . for the overhearing or recording of wire or oral communications," and similar language, which appeared throughout the First and Second Edition. Another set of changes resulted from a decision to remove from the Third Edition numerous references to applications and orders "approving the use" of emergency electronic surveillance. Standard 2-5.2 of the Second Edition, like its counterpart in the First Edition, permitted electronic surveillance to be employed in "an emergency situation" without a court order, but required that an application thereafter be made for an order "approving the use" of emergency surveillance. Standard 2-5.3 then set forth the requirements for an application for "an order authorizing or approving the use" of electronic surveillance (emphasis added), and the words "approving the use," or similar words, appeared repeatedly throughout the Standards. While the Third Edition retains provisions for emergency surveillance, see Standard 2-5.2, reference to an order "approving the use" of emergency electronic surveillance has been omitted from all the other Standards, because it was unnecessary and because including it to make explicit reference to those rare instances in which emergency surveillance is employed would have made the Standards complicated and unwieldy.²⁰


²⁰. The language was unnecessary. Standard 2-5.2(c) provides that when emergency electronic surveillance is conducted without a prior court order, an application must be made "for an order approving the interceptions to a judge with authority to issue an order authorizing the interceptions, had such an application been made." The application must not only establish to the court's satisfaction that the requisite emergency was present, but also that "there were grounds consistent with these standards upon which an order authorizing the electronic surveillance could have been issued." Standard 2-5.2(c)(v)(B). In other words, pursuant to Standard 2-5.2(c), an application for an order of approval must issue only when it meets all the requirements for an application prospectively authorizing the interception of communications pursuant to Standard 2.4.1, et seq. See also Standard 2-5.2(c)(iv) (also requiring for an order of approval that the communications intercepted during the emergency surveillance "were otherwise intercepted in accordance with these standards").
Standard 2-1.1. Objectives

The objectives of these standards are to assure the right to communicate privately, either in person or by technological means, and to determine under what conditions law enforcement, electronic communication service providers and other persons should be permitted to acquire, use and disclose such private communications.

Standard 2-2.1. Definitions

For purposes of these standards:
(a) A “communication” is:
   (i) any oral statement; or
   (ii) the transmission of any oral statement or of any signs, signals, writing, images, sounds, data or information of any nature, by wire, radio wave, or other technological means, including any statement or transmission to one’s self, but excluding any communication made through a tone-only paging device, or from a tracking device.
(b) A “private communication” is a communication which is made under circumstances in which a reasonable expectation of privacy exists. For these purposes, a reasonable expectation of privacy may
Electronic Surveillance of Private Communications

exist for a communication being transmitted by a communication service provider, or temporarily stored incident to that transmission, despite the fact that it is transmitted to more than one recipient, and despite the lawful access of the provider to the contents of that communication.

(c) "Electronic surveillance" is the non-consensual interception of the contents of a private communication by use of a mechanical, electronic or other device. For purposes of this definition:

(i) the "contents" of a communication are any information concerning the substance, purport, or meaning of that communication;

(ii) the contents of a private communication are "intercepted" when they are acquired contemporaneously with their transmission;

(iii) the contents of a communication are intercepted "non-consensually" when they are intercepted without the consent of at least one party to the communication; and

(iv) a "mechanical, electronic or other device" means any device or apparatus which can be used to intercept the contents of a private communication other than any instrument, equipment or facility, furnished to or by the subscriber to or user of an electronic communication service which is installed and used in the ordinary course of the subscriber's business; or by an investigative or law enforcement officer in the ordinary course of the officer's duties.

(d) "Minimization" is a good faith effort made to limit the interception of communications to those communications, or portions thereof, which are subject to interception pursuant to an electronic surveillance order.

(e) A communication is "subject to interception" if it is intercepted during lawfully conducted electronic surveillance and:

(i) it is evidence of an offense which is an authorized subject of the electronic surveillance, or of another offense; and

(ii) the communication is not privileged under applicable state law.

(f) "Law enforcement officer" means:

(i) any officer of the United States or of a state or one of its political subdivisions who is empowered by law to conduct an investigation of, or to make an arrest for, a criminal offense, and includes any agent of such an officer, and

(ii) any attorney authorized by law to prosecute or participate in the prosecution of such an offense.
(g) An "electronic communication service provider" is a person or entity which, in the ordinary course of business, routinely provides a service allowing its users to send or receive private communications, and a "public electronic communication service provider" is one who offers such a service to the public.

PART III.
GENERAL PRINCIPLES

Standard 2-3.1. General principles

The standards that follow incorporate and implement these general principles:

(a) The need to protect private communications.

(i) *Intrusion on private communications by the government.* The security of private communications from arbitrary intrusion by governmental officials is a basic necessity for the maintenance of a free society. Accordingly, law enforcement's authority to conduct electronic surveillance should be strictly regulated.

(ii) *Intrusion on private communications by others.* Because technology renders private communications vulnerable to interception by all persons, electronic surveillance by those outside law enforcement should also be strictly regulated.

(iii) *Protecting stored communications.* When technologically transmitted private communications are stored by an electronic communication service provider incidental to their transmission, access to those stored communications should also be regulated.

(iv) *Providing the same level of protection for all forms of communication.* Private communications should be afforded the same level of protection whether they are spoken in person or transmitted by technological means, and if by technological means, whether or not the communications include the human voice.

(b) The need to allow regulated electronic surveillance by law enforcement.

(i) *Need for electronic surveillance.* Because the interception of private communications can be an effective tool for the investigation and prosecution of criminal activity, law enforcement agencies should, in appropriate cases and under appropriate regulation, have
the legal authority and the technological means to conduct electronic surveillance, and to use the communications thus lawfully obtained, and evidence derived therefrom, in criminal and related civil actions.

(ii) *Balancing competing needs.* A proper balancing of privacy and law enforcement interests requires that electronic surveillance by law enforcement agencies be permitted only when:

(A) the objectives of an investigation are not likely attainable by alternative investigatory methods, and

(B) the intrusion is justified by the importance and likelihood of achieving those objectives.

(iii) *Constitutional requirements.* Except in emergency circumstances, electronic surveillance should be permitted only when authorized by a prior judicial order, which should be issued and executed in compliance with the Fourth Amendment requirements of probable cause, particularity, notice, and reasonableness.

(iv) *Non-constitutional requirements.* When law enforcement acquires a private communication non-consensually, the intrusion on privacy is greater if the contents are acquired contemporaneously with the transmission of the communication. Consequently, the use of electronic surveillance by law enforcement should be subjected to requirements beyond those mandated by the Fourth Amendment.

(v) *Regulating law enforcement’s access to stored communications.* Because the privacy interests in private communications stored incidental to their transmission are also significant, the law should also strictly regulate law enforcement’s authority to acquire and use the contents of such stored private communications.

(c) Applying for and executing an electronic surveillance order.

(i) *Establishing the necessity for electronic surveillance.* Electronic surveillance is an especially intrusive means of investigation. Accordingly, a judicial order authorizing a law enforcement officer to conduct electronic surveillance should be issued only when:

(A) the application for the order has been approved by a politically accountable prosecutor with the authority to establish and maintain a uniform electronic surveillance policy within the affected jurisdiction, or by a high ranking subordinate expressly authorized to exercise this responsibility;

(B) the applicant believes that the intrusion is justified by the importance and likelihood of achieving the objectives of the electronic surveillance; and
(C) the judge issuing the order approves the objectives of the electronic surveillance and finds that for purposes of achieving those objectives, other investigative procedures have been tried and have failed, or reasonably appear to be unlikely to succeed if tried or to be too dangerous.

(ii) *Employing the expertise required.* Officers executing an electronic surveillance order often must make complex legal determinations. Accordingly,

(A) the execution of such an order should be supervised by an attorney authorized to investigate and prosecute the crimes which are the subject of the order, and

(B) communications should be intercepted pursuant to the order by law enforcement officers who have been trained in the law and techniques of electronic surveillance, and who understand the terms and conditions of the order.

(iii) *Judicial monitoring of on-going electronic surveillance.* Because an electronic surveillance order is usually executed over an extended period of time, the judge who issues such an order can and should ensure that it is executed appropriately.

(iv) *Creating a reliable record.* To maximize the reliability of evidence obtained through the interception of private communications, a record of the contents of the communications thus intercepted should, whenever technologically possible, be made and preserved in a manner designed to protect its integrity.

(v) *Ensuring accountability.* To further ensure the accountability of law enforcement officials and officers who participate in electronic surveillance, law enforcement agencies should:

(A) promulgate administrative rules to ensure that the information necessary for such accountability exists;

(B) be subject to the exclusionary sanction in appropriate circumstances;

(C) promulgate internal regulations concerning the manner in which electronic surveillance is authorized and conducted;

(D) periodically review the scope and effectiveness of the electronic surveillance conducted; and

(E) maintain and make available to the public general information about the type or types of electronic surveillance conducted, and the frequency of their use.
PART IV.
COURT-ORDERED ELECTRONIC SURVEILLANCE

Standard 2-4.1. Order authorizing electronic surveillance; authorized application

(a) Except in an emergency situation, law enforcement officers should be permitted to conduct electronic surveillance only when authorized by a judicial order of the highest court of general trial jurisdiction, or a court authorized to hear appeals from that court.

(b) An application for such an order should be permitted:

(i) in the case of an order directed to a federal law enforcement officer, only when authorized by the Attorney General of the United States, or, when specifically permitted by Congress, by any other high ranking subordinate whom the Attorney General specially designates to authorize such applications, and who is either a presidential appointee or a person with appropriate expertise in applications for electronic surveillance orders; and

(ii) in the case of an order directed to a state or local law enforcement officer, only when authorized by the principal prosecuting attorney of the state or local government, or by a high ranking subordinate, when specifically permitted by state law and when specially designated by the principal prosecuting attorney to authorize such an application.

(c) A law enforcement officer should be permitted to conduct court-ordered electronic surveillance only when that officer is empowered by law to conduct an investigation of, or to make an arrest for, the particular offense as to which electronic surveillance is approved.

Standard 2-4.2. Application; form; contents; additional facts

(a) An application for an order authorizing the use of electronic surveillance should be made in writing upon an oath or affirmation and state:

(i) the identity of the prosecuting official authorizing the application pursuant to Standard 2-4.1(b);

(ii) the identity of the prosecuting attorney making the application;
(iii) the identity of the prosecuting attorney who will supervise the execution of the order;

(iv) the identity of the person, if known, whose communications are to be intercepted;

(v) the particular offense which is the subject of the electronic surveillance order;

(vi) the objectives of the electronic surveillance;

(vii) the particular kind of communications sought to be intercepted;

(viii) a particular description and the location of the facilities over which or the place where the communications are or will be occurring, or the facts demonstrating that specification of the facility or place is not practical;

(ix) the period of time for which eavesdropping authority is sought, including a statement that the authorization should not automatically terminate when the described type of communication has been first intercepted, if authority to intercept additional communications is sought;

(x) the material facts known to the applicant and necessary for the judge to determine whether the probable cause requirements set forth in Standard 2-4.3 have been satisfied;

(xi) the material facts necessary for the court to determine whether other investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or too dangerous;

(xii) the material facts known to those authorizing and making the application concerning such applications made within the past ten years for the authority to conduct electronic surveillance of the person whose communications are to be intercepted and the facilities over which or the place where the communications to be intercepted are or will be occurring, including, where the application is for the extension of an order, a statement setting forth the results thus far obtained from the electronic surveillance, or a reasonable explanation of the failure to obtain such results; and

(xiii) the need for particular electronic communication service providers and landlords, custodians, or other persons, if known, to furnish information, facilities, or technical assistance, if such is necessary in the execution of the order.

(b) The judge to whom the application is submitted should be permitted to require that additional facts be furnished under oath or affirmation, which should be duly recorded.
Standard 2-4.3. Probable cause; kinds of showings

The statements of facts relied upon and submitted by the applicant should establish:

(a) probable cause to believe that a person is committing, has committed, or is about to commit a particular designated offense;

(b) probable cause to believe that evidence concerning that particular offense may be obtained through electronic surveillance of the facilities over which or at the place where the communications to be intercepted are or will be occurring, unless, pursuant to Standard 2-4.10, the facility or place need not be specified;

(c) that for purposes of achieving the objectives of the electronic surveillance as described in the application, other investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous; and

(d) if the nature of the investigation is such that the authorization should not automatically terminate when the described type of communication has been first obtained, probable cause to believe that additional communications of the same type will occur thereafter.

Standard 2-4.4. Designated offenses; criteria

An application for an order authorizing electronic surveillance should be permitted only for the investigation of offenses which are punishable by more than one year imprisonment and have been designated by the legislature as serious enough to justify the intrusiveness of the surveillance.

Standard 2-4.5. Other offenses

(a) When, during lawfully conducted electronic surveillance, communications are intercepted which relate to offenses other than those specified in the initial surveillance order, whether or not those offenses are among the designated offenses for which such surveillance may be authorized, and the contents were obtained lawfully:

(i) the contents of those communications and evidence derived therefrom may be disclosed or used by law enforcement officers and officials to the extent such use or disclosure is appropriate to the proper performance of official duties; and

(ii) the contents of those communications and evidence derived therefrom may be introduced into evidence.
(b) When evidence of another designated offense has been intercepted, and the officers desire to obtain specific authority to intercept future communications relating to that offense, an application in conformity with Standards 2-4.1 through 2-4.4 should be made and approved.

(c) When evidence of another designated offense has been intercepted, and an application to intercept future communications constituting evidence of that offense has not been made pursuant to Standard 2-4.5(b), future communications relating to that other offense may nonetheless be intercepted in conformity with Standard 2-4.5(a).

**Standard 2-4.6. Judicial discretion and determination**

In the exercise of sound discretion:

(a) the judge to whom an application for authorization is submitted should be permitted to deny the application, and

(b) upon determining that the application satisfies the showings required by Standard 2-4.3, the judge should be authorized to grant the order either as requested, or with appropriate modifications, including but not limited to:

(i) reducing the length of the maximum period of authorized electronic surveillance;

(ii) modifying the authorized objectives of the electronic surveillance;

(iii) requiring progress reports, or modifying the frequency with which progress reports, if any, must be submitted;

(iv) specifying or modifying the manner in which records of intercepted communications are to be made;

(v) specifying or modifying the manner in which the minimization of communications not subject to interception is to be achieved, either contemporaneously with or after their interception; or

(vi) when the authorization sought is to intercept communications occurring in more than one place and/or over more than one facility, granting only part of the authority requested.

**Standard 2-4.7. Order; jurisdiction**

(a) A federal judge should be permitted to issue an electronic surveillance order authorizing the interception of private communications, regardless of where those communications are occurring, if the
communications are to be intercepted in the United States, and the
offense which is the authorized subject of the electronic surveillance
has been, is being, or is about to be committed within the territorial
jurisdiction of the court; and

(b) A state judge should be permitted to issue an order authorizing
the interception of private communications, regardless of where
those communications are occurring, if:

(i) the offense which is the authorized subject of the electronic
surveillance has been, is being, or is about to be committed within
the territorial jurisdiction of the court in which the judge is sitting,
and the communications are to be intercepted within the state; or

(ii) the offense which is the authorized subject of the electronic
surveillance has been, is being, or is about to be committed in another
state; the communications are to be intercepted within the territorial
jurisdiction of the court in which the judge is sitting; and the law
of the state in which the judge sits permits the judge to issue such
an order;

provided, however, that:

(iii) a state court judge should be permitted to issue an order
authorizing the interception of communications occurring between
or among parties known to be outside the state only pursuant to
an interstate compact permitting such interceptions; and

(iv) an electronic communication service provider should be
required to comply with an order issued pursuant to Standard
2-4.8(i) that it furnish information, facilities, or technical assistance
for the execution of an electronic surveillance order to be executed in
a state if:

(A) the provider is lawfully served with the order in that state, or
(B) the provider is lawfully served with the order in another
state and is required to comply with it pursuant to an interstate
compact.

Standard 2-4.8. Order; form; contents

The order should be issued in writing signed by the judge and con­tain
the following information:

(a) the identity of the prosecuting official authorizing the applica­tion pursuant to Standard 2-4.1(b);

(b) the identity of the prosecuting attorney who will supervise the
execution of the order;
(c) the identity of the agency employing the law enforcement officers authorized to intercept communications;
(d) the identity of the person, if known, whose communications are to be intercepted;
(e) a specification of the particular offense as to which electronic surveillance is approved;
(f) a particular description of the communications sought to be intercepted;
(g) a particular description of the facilities from which or the place where the communications to be intercepted are or will be occurring, unless the order is issued pursuant to Standard 2-4.10;
(h) a directive that the interception of communications shall begin at a specified time or as soon as practicable, and in any case, no later than ten days after the order is issued;
(i) where requested and approved, a directive requiring electronic communication service providers, landlords, custodians, or other persons to furnish information, facilities, or technical assistance, and authorizing compensation for the costs of such assistance;
(j) a directive that minimization of the intercepted communications be accomplished contemporaneously with their interception;
(k) a statement of the maximum period of authorized electronic surveillance, which shall not be longer than warranted by the showings of probable cause required by subdivisions (a) and (b) of Standard 2-4.3, and in any event, not longer than thirty days from the time specified for the beginning of interception of communications;
(l) a directive that the interception of communications shall terminate upon the accomplishment of the objectives of the electronic surveillance, as those objectives are set forth in the application pursuant to Standard 2-4.2(a)(vi), and are approved by the court; and
(m) a directive that the prosecuting attorney the application states will supervise the execution of the order, or another prosecuting attorney acting on his or her behalf, must supervise the execution of the order, and, unless the authorized period of electronic surveillance is ten days or less, periodically submit progress reports to the court containing:
(i) information reasonably adequate to permit the judge to review whether the order is being executed in a manner which minimizes the interception of communications not otherwise subject to interception, and whether continued interception of the communications pursuant to the order is necessary to achieve the objectives of the
Electronic Surveillance of Private Communications

2-4.8

electronic surveillance, as those objectives are set forth in the appli­cation pursuant to Standard 2-4.2(a)(vi) and approved by the court pursuant to Standard 2-4.8(l);

(ii) notice of the interception and content of any communication, if known, that does not relate to an offense specified in the elec­tronic surveillance order, but does relate to another offense not specified in that order, and

(iii) identification, by number or otherwise, of the records made of the contents of the intercepted communications pursuant to Standard 2-4.14.

Standard 2-4.9. Minimization after communications intercepted

(a) When it is not reasonably possible to satisfy the minimization requirement of Standard 2-4.8(j), either because the technological means by which the intercepted communications are transmitted do not permit it, or because the intercepted communications are in a code or foreign language which cannot reasonably be deciphered or trans­lated at the time of interception, the minimization requirement set forth in that standard should be considered satisfied if:

(i) a law enforcement officer who is familiar with the investiga­tion of the offense for which the electronic surveillance is autho­rized, or an individual acting under the supervision of such a law enforcement officer, accomplishes that minimization as soon as practicable after the communications are intercepted;

(ii) to the extent reasonable and possible, that minimization is accomplished in a manner designed to protect the privacy inter­ests of the parties to the communications to the same extent as properly conducted contemporaneous minimization, had contemporaneous minimization been possible;

(iii) the minimizing officer, or the individual acting under his supervision, makes at least one original record of the communica­tions that the officer determines were otherwise subject to inter­ception, for disclosure to and use by the other law enforcement officers participating in the investigation;

(iv) the minimizing officer preserves an original record of the communications made as they were intercepted and before they were minimized, along with any other original or duplicate of the record used to accomplish the minimization, using procedures designed to prevent others from having access to the contents of the record; and
(v) the contents of the communications that the minimizing officer determines were not otherwise subject to interception are not otherwise disclosed, except as authorized by judicial order.

(b) When the electronic surveillance order does not already authorize such minimization procedures, the judge who issued the order should be notified, in the next progress report or application for an extended electronic surveillance order, whichever is earlier, that such procedures are being employed.

(c) Whenever progress reports are filed, and within five days after the end of the authorized period of electronic surveillance, the issuing judge should be presented with the original records of the communications thus far preserved by the minimizing officer pursuant to subdivision (a)(iv), and not yet presented to the judge. Those records should be maintained in a place specified by the judge under such conditions as the judge may order, and that place and those conditions should not be changed except by judicial order.

Standard 2-4.10. Order not specifying place or facilities; application and authorization

An order which does not particularly describe the location of the facilities from which or the place where the communications to be intercepted are or will be occurring, may be issued if:

(a) the order otherwise complies with the requirements of Standard 2-4.8;

(b) the application for the order contains a full and complete statement demonstrating that specification of a facility or place is not practical;

(c) the judge issuing the order finds from the application probable cause to believe that such specification is not practical;

(d) the application identifies one or more persons committing the offense; and

(e) the authorization to intercept communications is limited to the interception of communications of the person or persons so identified.

Standard 2-4.11. Extensions

Extensions of an order authorizing electronic surveillance should be granted for periods of not longer than thirty days upon filing and approval of an application in accordance with Standards 2-4.1, 2-4.2,
2-4.3, 2-4.4, and, when applicable, 2-4.10. No limit should be placed on the number of extensions that may be granted. In the exercise of sound discretion, an application for such an extension may be denied, or granted as requested or with appropriate modifications, in accordance with Standard 2-4.6.

Standard 2-4.12. Privileged communications

(a) No order should be permitted authorizing interception of communications over a facility or in a place primarily used by professionals whose communications are privileged under applicable state law, or in a place used primarily for habitation by a husband and wife, unless, in addition to the showings required under Standard 2.4.3, and, where applicable 2-4.10, the applicant establishes probable cause to believe that there is a particular need to conduct such surveillance over that facility or in that place.

(b) No otherwise privileged communication intercepted in accordance with or in violation of these standards should lose its privileged character.

Standard 2-4.13. Orders and applications; custody; destruction

All orders and applications should be maintained in such places as the judge directs. Orders and applications may be destroyed ten years after they are issued, and may be destroyed earlier when the judge so directs. Orders and applications should not be disclosed except as authorized by statute or judicial order.


(a) At least one original record of the contents of any communications intercepted by electronic surveillance should be made contemporaneously with its interception.

(b) To the extent possible and reasonable given the form of the communications and the available technology, the equipment and techniques used to make the record should:

(i) enable the intercepting officers to make a complete and accurate record of the intercepted communications, and
(ii) either protect an original record from editing or other alteration, or disclose whether that record has been edited or altered.

(c) If such equipment and techniques are used, but fail to make an original record of a particular communication, the law enforcement officer intercepting the communication should transcribe the communication as accurately as possible, and the issuing judge should be notified of the failure and provided with a copy of the transcript no later than the next progress report, or within five days of the end of the authorized period of eavesdropping.

(d) When communications are minimized contemporaneously with their interception, an intercepting officer should take steps to preserve one original record of the intercepted communications immediately after the record is completed, following procedures designed to protect it from editing or alteration.

(e) When communications are minimized after they are intercepted pursuant to Standard 2-4.9, in addition to preserving, as required by Standard 2-4.9(a)(iv), an original record of the communications made as they were intercepted and before they were minimized, the minimizing officer should also take steps to preserve one original record of the minimized communications made pursuant to Standard 2-4.9(a)(iii) immediately after the minimization is accomplished, following procedures designed to protect the record from editing or alteration.

(f) Under appropriate safeguards, other copies of those records, whether original or duplicate, may be made, used and disclosed for investigative purposes or trial preparation.

Standard 2-4.15. Inventory; contents; time; postponement

(a) After the authorization for electronic surveillance, including any extension of that authorization, has ended, the judge should order that an inventory be served on:

(i) the persons named in the order of authorization, and

(ii) any other identified parties to the intercepted communications whom the judge determines should be served in the interest of justice.

(b) The inventory should include notice of:

(i) the entry of the order;

(ii) the date of the entry of the order;

(iii) the period of authorized electronic surveillance;
(iv) the interception, if any, of communications; and
(v) the period, if any, of actual interception of communications.

(c) The judge should order that the inventory be served as soon as practicable, and no later than a specified date, not less than thirty days and not more than ninety days after the authorization for electronic surveillance, including any extension of that authorization, has ended. Upon a showing of good cause made to the judge, the date should be postponed.

(d) Upon application of a person who has received such an inventory, and on notice to the applicant for the electronic surveillance order, the judge may order further disclosure if the judge finds such disclosure is required in the interest of justice.

Standard 2-4.16. Disclosure; use

(a) A law enforcement officer should be permitted to disclose, receive or use the contents of a private communication intercepted by means of electronic surveillance conducted in a manner authorized by these standards, or evidence derived therefrom, only to the extent it is in the proper performance of the officer's official duties.

(b) Any person who is not a law enforcement officer should be permitted to disclose or use such a communication if the person obtains the contents of the communication lawfully and uses or discloses it for any lawful purpose.

Standard 2-4.17. Reports

(a) Judges should make annual reports concerning electronic surveillance orders to an appropriate agency which should contain:

(i) the number of orders applied for;
(ii) the kinds of orders applied for;
(iii) the number of orders denied, the number granted as applied for, and the number granted as modified;
(iv) the periods of time over which electronic surveillance was conducted or records were made pursuant to each electronic surveillance order, including each extension of such an order;
(v) the offenses specified in the orders or the applications which were denied;
(vi) the identity of the persons authorizing the applications; and
(vii) the identity of the law enforcement agency of the applicant.
(b) Applicants should make annual reports concerning their applications to the agency specified in paragraph (a) which should contain:

(i) the information required in subdivisions (a)(i)-(vii);
(ii) a general description of the intercepting, separated by offense, including:

(A) the character and frequency of the incriminating communications intercepted;
(B) the character and frequency of the other communications intercepted;
(C) the number of persons whose communications were intercepted; and
(D) the character and amount of manpower and other resources used in the intercepting;
(iii) the number of arrests resulting from the intercepting;
(iv) the offenses for which the arrests were made;
(v) the number of trials in which intercepted communications, or evidence derived from intercepted communications, was used;
(vi) the number of motions to suppress made, granted, or denied based on the intercepting;
(vii) the number of convictions in cases in which intercepted communications, or evidence derived from intercepted communications, was used; and
(viii) the offenses for which the convictions were obtained.

(c) The agency specified in subdivisions (a) and (b) should make public a complete annual report based on the information required to be filed by subdivisions (a) and (b).

PART V.
INTERCEPTION OF COMMUNICATIONS BY LAW ENFORCEMENT WITHOUT AN ELECTRONIC SURVEILLANCE ORDER

Standard 2-5.1. Intercepting communications with consent

(a) A law enforcement officer should be permitted to intercept the contents of a private communication with the consent of one of the par-
ties to the communication without a court order, provided that the officer intercepts and uses the communication in the proper performance of the officer’s official duties.

(b) A law enforcement officer should be permitted to intercept the contents of the communications of an unauthorized user of an electronic communication service provider to or over that service without a court order when:

(i) the provider reasonably determines that the communications threaten to disrupt the provider’s service; and

(ii) the provider consents to the interception, provided that the officer intercepts and uses the communications in the proper performance of the officer’s duties.

(c) When a law enforcement officer intercepts the contents of a private communication with the consent of one of the parties to the communication pursuant to subdivision (a), or with the consent of an electronic communication service provider pursuant to subdivision (b), the officer should record it whenever reasonably possible and appropriate to do so, employing devices and techniques which will ensure that the record will be, insofar as practicable, complete and accurate. Administrative procedures should be followed in determining when it is not appropriate to make such a record, and when a record is made, procedures similar to those set forth in Standards 2-4.14, and 2-7.1 should be followed.

Standard 2-5.2. Intercepting communications in an emergency situation

(a) When a law enforcement officer reasonably believes that an emergency situation exists which involves substantial and imminent danger to human life, the officer should be permitted to conduct electronic surveillance without a prior judicial order when:

(i) the law enforcement officer is authorized to intercept those communications:

(A) in the case of a federal law enforcement officer, by the Attorney General, the Deputy Attorney General or the Associate Attorney General; or

(B) in the case of a state or local law enforcement officer, by the principal prosecuting attorney of the state or local government, or by a high ranking subordinate, when specifically permitted by
state law and when specially designated by the principal prosecuting attorney to authorize the interception of communications in such a situation; and
(ii) the prosecuting official authorizing the interceptions pursuant to subdivision (i) first determines:
(A) that there are grounds consistent with these standards upon which an order could be obtained authorizing an interception; and
(B) because of the emergency, it is not practicable to make an application for such an order before the communications are intercepted.

(b) The requirements of making and protecting the integrity of a record of the contents of the communications, set forth in Standard 2-4.14, shall be followed during any period of emergency surveillance.

(c) Communications intercepted in conformance with Standard 2-5.2(a) may be disclosed and used in accordance with Standard 2-4.16 when:
(i) the prosecuting officer who authorized the interceptions, or when that officer is absent or unavailable, another prosecuting officer who could have authorized the interceptions pursuant to Standard 2-5.2(a)(i), makes an application for an order approving the interceptions to a judge with authority to issue an order authorizing the interceptions, had such an application been made;
(ii) the application sets forth the material facts upon which the prosecuting officer relied in authorizing the interceptions;
(iii) the application is made within a reasonable period of time but not more than forty-eight hours after the interception of communications has begun;
(iv) the communications were otherwise intercepted in accordance with these standards; and
(v) the judge to whom the application is made approves the interceptions based upon a determination that the application demonstrates that, at the time the prosecuting officer authorized the interceptions:
(A) the law enforcement officer reasonably believed he was confronted with the requisite emergency situation; and
(B) there were grounds consistent with these standards upon which an order authorizing the electronic surveillance could have been issued.
2-5.2  

Electronic Surveillance of Private Communications

(vi) The judge to whom the application is made should be permitted to require the furnishing of additional facts under oath or information, which should be duly recorded.

(d) Unless an application for approval is made and granted, the intercepted communications should be treated as impermissibly obtained pursuant to Standard 2-6.2(a) and an inventory filed as provided in Standard 2-4.15.

PART VI.
SANCTIONS

Standard 2-6.1.  Sanctions, in general

Except as otherwise permitted by these standards, electronic surveillance by any person should be expressly prohibited, and this prohibition should be enforced with appropriate criminal, civil, and evidentiary sanctions.

Standard 2-6.2.  Evidentiary sanctions; exceptions

(a) Except as otherwise expressly permitted under these standards, a private communication intercepted by a law enforcement officer by means of electronic surveillance, and any evidence derived therefrom, should not be received in evidence in any trial, hearing, or proceeding in or before any court, grand jury, department, officer, agency, regulatory body, or other authority.

(b) When a law enforcement officer intercepts a private communication by means of electronic surveillance conducted in a manner not expressly permitted by these standards, the communication, and any evidence derived therefrom, may nonetheless be received in evidence:

(i) in a prosecution for the unlawful interception of that communication; or

(ii) if the intercepted communication, or evidence derived therefrom, includes exculpatory information, and the defendant offers it in evidence, provided, however, that in response, the prosecution may offer evidence of, or derived from, that communication or
another communication, if it would tend to rebut the evidence offered by the defendant pursuant to this subdivision.

(c) When a prosecuting attorney intends to offer evidence of the contents of communications obtained by a law enforcement officer by means of electronic surveillance, or evidence derived therefrom, the prosecuting attorney should give notice of that intention within a reasonable period before trial, and should disclose to the defendant at that time:

(i) the order or orders pursuant to which the electronic surveillance was conducted;
(ii) the applications for those orders;
(iii) the progress reports submitted to the court pursuant to those orders;
(iv) copies of the records of the communications the prosecuting attorney intends to offer in evidence; and
(v) such other material as may be required by the judge before whom the suppression motion referred to in subdivision (f) is made for purposes of the motion.

(d) For the purpose of protecting the privacy of any person who is not a subject of the prosecution, the court may, upon the application of the prosecuting attorney or the defendant, or sua sponte, issue a protective order prohibiting or regulating the disclosure to others of the contents of these materials.

(e) When the prosecutor gives notice pursuant to subdivision (c) of this standard of the intent to offer evidence obtained by means of electronic surveillance, if communications obtained by the electronic surveillance were minimized pursuant to Standard 2-4.9:

(i) the court should order that the communications that the minimizing officer determined were not otherwise subject to interception be disclosed to the defendant;
(ii) if the defendant intends to offer in evidence the contents of any of those communications in any proceeding, the defendant should give notice of that intention to the prosecutor within a reasonable period of time before the proceeding;
(iii) if the defendant gives such notice, the court should order, upon request of the prosecutor, that the communications disclosed to the defendant pursuant to subdivision (i) be disclosed to the prosecutor; and
(iv) when communications are disclosed to the defendant pursuant to subdivision (i), or to the prosecutor pursuant to subdivi-
sion (iii), the court should issue a protective order prohibiting or regulating the disclosure of those communications to others.

(f) Any party aggrieved by the interception, use, or disclosure of private communications by law enforcement, or of evidence derived therefrom, otherwise than as expressly permitted under these standards, should be permitted to move to suppress those communications or that evidence. The motion should be made prior to the trial, hearing, or other proceeding unless there was no opportunity to make the motion or the party was unaware of the grounds on which the motion could be made. Where such a motion is made and granted, prior to the attaching of jeopardy, during the course of a criminal prosecution, the prosecuting attorney, where necessary, should be afforded a right of appeal provided that the appeal is not taken for the purpose of delay and is diligently prosecuted.

(g) Such evidence should be suppressed if:

(i) the communications were obtained in violation of the Constitution of the United States, or, in the case of an order issued by a state or local judge, of the state constitution;

(ii) the communications were obtained pursuant to an order issued by a judge other than as permitted by Standard 2-4.1, or upon an application made by an applicant other than as permitted by Standard 2-4.2, or upon an application failing to make one of the showings required by Standard 2-4.3; or

(iii) the evidence is obtained in violation of a statutory provision designed to enforce one of the general principles set forth in these standards governing electronic surveillance, unless the violation was committed in reasonable reliance upon an electronic surveillance order.

(h) When a person who is not a law enforcement officer intercepts the contents of a private communication in a manner not authorized pursuant to these standards or prohibited by law, a law enforcement officer should not be permitted to receive and use that communication unless:

(i) the person who intercepts the communication does not do so as an agent of a law enforcement officer;

(ii) the officer receives and uses the communication in the proper performance of the officer's duties; and

(iii) the communication is used with respect to a crime in which physical injury to a person or serious physical damage to property is caused or threatened.
In exercising discretion to use a communication so intercepted in a criminal prosecution, the prosecuting attorney should consider the manner in which the communication was obtained and the effect of its use on privacy.

Standard 2-6.3. Criminal sanctions

(a) The possession, sale, distribution, advertisement, and manufacture of devices primarily useful for the surreptitious interception of private communications should be regulated in order to prevent the use of such devices in a manner not authorized by these standards.

(b) The following conduct should be made criminal:

(i) the intentional interception of private communications by means of electronic surveillance conducted in a manner not authorized by these standards;

(ii) the intentional use or disclosure of private communications intercepted by means of electronic surveillance, or evidence derived therefrom, when the electronic surveillance is conducted in a manner not authorized by these standards, or when the communications are used or disclosed in such an unauthorized manner;

(iii) the possession, sale, distribution, advertisement, or manufacture of a device primarily useful for the surreptitious interception of private communications in violation of a regulation adopted pursuant to Standard 2-6.3(a); and

(iv) the intentional promotion, whether by advertising or otherwise, of any device for use in intercepting such communications in a manner not authorized by these standards.

(c) Any device possessed, used, sold, distributed, or manufactured in violation of these prohibitions or regulations should be subject to confiscation.

Standard 2-6.4. Civil sanctions

(a) Except as otherwise expressly permitted by these standards, the use of electronic surveillance, or the use or disclosure of a communication intercepted by means of electronic surveillance, or evidence derived therefrom, should give rise to a civil cause of action against any person or governmental agency who so conducts the electronic
surveillance, or knowing or having reason to know that such com-
munication or evidence was obtained by electronic surveillance, who
so discloses or uses such communication or evidence derived there-
from, or procures or authorizes another to do so.

(b) Good faith reliance on a court order or other legislative autho-
rization should constitute a complete defense to civil recovery.

PART VII:
ADMINISTRATIVE REGULATIONS

Standard 2-7.1. Administrative regulations

(a) Law enforcement agencies should adopt administrative regu-
lations, including standards, procedures, and sanctions, dealing with
the various aspects of the use of electronic surveillance techniques.
The regulations, among other things, should:

(i) limit the number of officers in the agency authorized to
employ the techniques;

(ii) specify the circumstances under which the techniques may
be used, giving preference to those which invade privacy least;

(iii) set out the manner in which the techniques must be used to
assure authenticity;

(iv) require that officers who execute electronic surveillance
orders first be trained in the law and techniques of electronic sur-
veillance;

(v) require the close supervision of officers authorized to employ
the techniques;

(vi) permit an officer to execute an order authorizing electronic
surveillance only after the officer has read the order and the
application, and has been instructed by the prosecuting attorney
concerning the crime for which electronic surveillance has been
authorized, the objectives of the electronic surveillance, the parties
whose communications may be intercepted, the types of commu-
nications which may be intercepted, and the obligation to mini-
mize the interception of communications which are not otherwise
subject to interception;

(vii) circumscribe the acquisition of, custody of, and access to
electronic equipment by agents; and
Electronic Surveillance of Private Communications

2-8.1

(viii) restrict the transcription of, custody of, and access to overheard or recorded communications by agents.

(b) Materials on the regulations should be incorporated into general and special training programs of the agency.

PART VIII.
PRIVATE COMMUNICATIONS ACQUIRED BY AND RECEIVED FROM ELECTRONIC COMMUNICATION SERVICE PROVIDERS

Standard 2-8.1. Communications acquired by an electronic communication service provider

(a) An electronic communication service provider not offering its services to the public, and the principals, employees and agents of such a provider, should be permitted to acquire, use and disclose the contents of the private communications transmitted over or stored with its service for any lawful purpose.

(b) A public electronic communication service provider, and its principals, employees and agents, should be permitted to acquire, use and disclose the contents of the private communications of its customers and other authorized and unauthorized users only:

(i) to the extent necessary to render the service, and to maintain and protect the availability, integrity and confidentiality of the system; or

(ii) in the case of a stored communication:

(A) to the sender or an intended receiver of the communication, or an agent of the sender or an intended receiver; or

(B) with the consent of the sender or an intended receiver of the communication; or

(iii) to a law enforcement officer:

(A) if otherwise authorized by these standards, or

(B) if the public electronic communication service provider obtained the contents of the communication in a manner permitted by these standards, or obtained them inadvertently, and the communication appears to pertain to the commission of a crime.
Standard 2-8.2. Communications received by law enforcement from an electronic communication service provider

(a) A law enforcement officer should be permitted to receive the contents of a private communication from an electronic communication service provider when:

(i) the communication is evidence of a crime and was lawfully acquired by the provider;

(ii) the communication has been in storage with the provider, either temporarily and incidental to its transmission, or for purposes of its backup protection, and is obtained pursuant to a search warrant directing the provider to disclose the communication based on the application of an appropriate law enforcement official establishing probable cause to believe that the communication constitutes evidence of a crime; or

(iii) the communication has been in storage with the provider for more than 45 days, either temporarily and incidental to its transmission, or for purposes of its backup protection, and is obtained pursuant to a trial, grand jury or administrative subpoena authorized by federal or state law, or pursuant to a court order issued upon the application of a prosecuting attorney establishing reasonable grounds to believe that the contents of the communication are relevant and material to an ongoing criminal investigation.

(b) When an application for a search warrant is made pursuant to Standard 2-8.2(a)(ii), the applicant should be required to inform the judge from whom the warrant is sought of any previous applications made by or known to the applicant for a warrant requiring the disclosure of stored communications of the same customer.

(c) When an electronic communication service provider discloses private communications to a law enforcement officer:

(i) the law enforcement agency to which the disclosure is made should be required to give prior notice of the disclosure to the customer if the disclosure is made pursuant to a trial, grand jury or administrative subpoena, or pursuant to a court order, provided that a court may postpone such notice upon a showing of good cause; and

(ii) based upon a showing of good cause, a court may prohibit the provider from notifying the customer of the disclosure.

(d) Upon the written request of a law enforcement officer or prosecuting attorney, an electronic communication service provider should
be required to take all necessary steps to preserve a record of the contents of a stored electronic communication pending the issuance of a court order or subpoena. If such a request is made, the provider should be required to preserve the record for ninety days. Upon a renewed written request by the prosecuting attorney, the provider should be required to preserve the record for an additional ninety days.

(e) A law enforcement officer should be permitted to disclose, receive or use the contents of a private communication which the officer has obtained from an electronic communication service provider by means authorized by these standards, or evidence derived therefrom, only to the extent it is in the proper performance of the officer's official duties.

Standard 2-8.3. Communications received by other persons from an electronic communication service provider.

A person who is not a law enforcement officer:

(a) should be prohibited from obtaining from an electronic communication service provider the contents of a private communication stored with that provider unless disclosure of that communication by the provider to that person is permitted by these standards or is otherwise lawful; and

(b) should be permitted to disclose or use the contents of such a communication if the person obtains the contents of the communication lawfully and uses or discloses it for any lawful purpose.
Standard 2-1.1. Objectives

The objectives of these standards are to assure the right to communicate privately, either in person or by technological means, and to determine under what conditions law enforcement, electronic communication service providers and other persons should be permitted to acquire, use and disclose such private communications.

Commentary to Standard 2-1.1

Both the First and Second Edition of the Standards announce that "[t]he objectives of standards relating to the use of electronic surveillance techniques should be the maintenance of privacy and the promotion of justice." While this statement of objectives was noble in tone, it was too general to provide substantive guidance for the Standards that follow. First, a proclamation about the importance of maintaining "privacy" failed to identify the particular privacy interest at stake in the regula-
tion of electronic surveillance. Second, and more importantly, juxtapos-
ing "the maintenance of privacy" with "the promotion of justice" raised
questions as to meaning of "justice." If justice is promoted exclusively by
permitting law enforcement to use electronic surveillance as an investi-
gative and prosecutorial tool, then justice can be promoted only at the
expense of privacy. If, however, justice is also promoted when regula-
tions are created and enforced that limit when and how electronic sur-
veillance may be used, then maintaining privacy and promoting justice
are not—or at least are not always—inconsistent goals. Moreover, this
juxtaposition of privacy and justice could be misconstrued as a sugges-
tion that the threat to the privacy of communications comes exclusively
from the government, and not from those who provide communication
services and others who, without governmental sanction or assistance,
engage in electronic surveillance.

To remove these ambiguities, the Third Edition begins with a state-
ment that—while perhaps less noble in tone—is more specifically
directed to the purposes of the Standards. It specifies that when elec-
tronic surveillance is employed, a particular kind of privacy right is at
stake: "the right to communicate privately, either in person or by tech-
nological means." And it sets forth more precisely what the Standards
that follow attempt to achieve, that is, striking the appropriate balance
between the privacy of communications and the legitimate interests of
law enforcement and service providers, "by determining under what
conditions law enforcement, electronic communication service providers
and other persons should be permitted to acquire, use and disclose . . .
private communications."2

2. Indeed, the public interest lies in striking the appropriate balance among these
interests, and it would be unfair to suggest that the relationship among them is com-
pletely adversarial. Law enforcement agents seek to conduct electronic surveillance on the
public's behalf—that is, to protect the public safety. Similarly, although communication
service providers do have business interests to protect (e.g., a provider may monitor a
hacker to protect a service that generates revenue), they also share a role in protecting
the public from the transmission of threatening e-mails and the distribution of child
pornography.
PART II.
DEFINITIONS

Standard 2-2.1. Definitions

Commentary to Standard 2-2.1

The First and Second Edition of the Standards did not include a set of definitions. They were added to the Third Edition to clarify the meaning of terms, resolve any ambiguity in their reach and meaning resulting either from case law or from developments in technology, and to simplify the language of the subsequent Standards in which these terms are employed.

For purposes of these standards:
(a) A "communication" is:
   (i) any oral statement; or
   (ii) the transmission of any oral statement or of any signs, signals, writing, images, sounds, data or information of any nature, by wire, radio wave, or other technological means, including any statement or transmission to one’s self, but excluding any communication made through a tone-only paging device, or from a tracking device.

Commentary to Standard 2-2.1(a)

The Third Edition of the Standards contains definitions that are designed to identify the types of communications that are covered.
   (a) A "communication." Included within the term "communication" are two kinds of "oral statement[s]": those a person utters face to face, or those transmitted by means of any telephonic or other technological means. A "communication" also includes any electronic communication, that is, "the transmission . . . of any signs, signals, writing, images, sounds, data or information of any nature, by wire, radio wave, or other technological means." Title III does not include an overarching definition for a "communication," but instead separately defines the terms "wire communication," "oral communication" and "electronic communication." The separate definition of these terms is significant, since Title III provides more protection for "wire" and "oral" communications than it does for "electronic" ones. The merger in Standard 2-2.1(a) of all three
kinds of communications in a single unified definition is equally significant, since it signals the intent of the Standards to extend the same level of protection to all three. See the commentary to Standard 2-3.1(a)(iv).

Title III does not define an "oral communication" as a communication between one person and another, and while it defines "electronic" and "wire communication[s]" as "transfer[s]" of data or the human voice, it also does not specify whether the data or voice must be transferred from one person to another. While it has been argued that, implicitly, a "communication" must have more than one party, a person who transmits a message or data to himself or herself may have a greater expectation of privacy than someone who communicates with another, since in the latter case, the person has not only provided information to someone else, but also risks that the other person will disclose that information to others. Because the definition of "communication" in Standard 2-2.1(a) includes "any statement or transmission to one's self" it makes explicit that such statements and transfers are protected, for example, when a person leaves himself or herself a message by phone or e-mail, transmits a document from a home computer to one at work, or merely talks aloud when alone.

Standard 2-2.1(a) excludes from the term "communication" one "made through a tone-only paging device, or from a tracking device." This exclusion mirrors 18 U.S.C. § 2510(12)(B) and (C), which also exclude such communications from Title III's definition of an "electronic communication."

3. No court has yet determined whether a technological transfer of voice or sound from one person to himself or herself is a "communication" protected by Title III, but in a related context, one court, pointing to the definition of the term in Webster's Ninth New Collegiate Dictionary (1984) as "a process by which information is exchanged between individuals through a common system of symbols, signs, or behavior," concluded that, "[i]f it takes two to tango, it takes at least two to communicate." In re Askin v. McNulty, 47 F.3d 100, 104 (4th Cir. 1995).

4. See United States v. Turk, 526 F.2d 654, 658, n.2 (5th Cir. 1976) in which the court observed, "In a forest devoid of listening listeners, a tree falls. Is there a sound? The answer is yes, if an active tape recorder is present, and the sound might be thought of as 'aurally acquired' at (almost) the instant the action causing it occurred."

5. Subdivision (A) of § 2510(12)(A) also excludes "any wire or oral communication" from the term "electronic communication," but this exclusion is unnecessary in Standard 2-2.1(a), which defines the term "communication" without regard to whether, in the language of Title III, the communication is an "oral," "wire" or "electronic" one. Subdivision
(i) An "oral statement." While Standard 2-2.1(a)(1) defines a communication as including face to face "oral statement[s]," Title III defines an "oral communication" as "any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying that expectation . . . ." 18 U.S.C. § 2510 (2). The federal definition obviously makes no attempt to delineate what an "oral communication" is, but is instead intended only to limit Title III's protections to oral communications that are subjectively and objectively private. Since the Standards offer protection only to "private" communications, and since Standard 2-2.1(b) defines a "private communication" as "a communication which is made under circumstances in which a reasonable expectation of privacy exists," an "oral statement" that is "private" within the meaning of the Standards is an "oral communication" within the meaning of Title III.

(ii) The transmission of an "oral statement." While Standard 2-2.1(a)(2) defines a communication as including "[t]he transmission of any oral statement . . . by wire, radio wave, or other technological means," Title III defines a "wire communication" as "any oral transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of communications . . . ." 18 U.S.C. 2510(1). In light of on-going developments in the wireless transmission of communications, the Standards define the term "communication" independent of Title III's requirement that the communication be transmitted at any point "by the aid of wire, cable or other like connection."

Although ECPA does not include a stored electronic communication within the definition of an "electronic communication," 18 U.S.C. § 2510(12), until recently it defined a "wire communication" to include a stored communication containing the human voice [i.e., an aural communication]. 18 U.S.C. 2510(1). Thus a stored "wire communication"—for

(D) of § 2510(12)(A) also excludes from an "electronic communication" "electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds." The Standards do not consider whether such information, like other transactional information, should be excluded from its definition of the term "communication," and the omission of that exclusion from the Standards should not be considered as a statement that such information should be included.
example, a message containing the human voice recorded by a voice mail system—was given the full protection of Title III, while a stored electronic communication—for example, e-mail stored with a service provider—is not. Consistent with the general principal set forth in Standard 2-3.1 that "[p]rivate communications should be afforded the same level of protection . . . whether or not the communication includes the human voice," Standard 2-2.1(a) rejects a definition of a "communication" that would distinguish between stored "wire communications" (which, by definition, include the human voice) and those that are electronic (which, by definition, do not). And by excluding stored communications—both aural and electronic—from the definition of a "communication," Standard 2-2.1(a) recognizes that stored communications do not deserve the full level of protection afforded to communications while still in transmission, because the storage of a communication lowers, to some degree, the expectation of privacy in a communication that would otherwise be ephemeral in nature. In the USA PATRIOT Act, Congress adopted the approach of the Standards, distinguishing stored wired communication from wire communications in transmission, and permitting stored wired communications to be obtained as stored electronic communications can, without an electronic surveillance order.

(b) A "private communication" is a communication which is made under circumstances in which a reasonable expectation of privacy exists. For these purposes, a reasonable expectation of privacy may exist for a communication being transmitted by a communication service provider, or temporarily stored incident to that transmission, despite the

---

6. In United States v. Smith, 155 F.3d 1051 (9th Cir. 1998), the court relied in part on this distinction in holding that when one person accessed another person's voice mailbox without authorization, forwarded to herself one of the voice communications stored in the mailbox, and then played it and recorded it with a hand held tape recorder, she intercepted the communication in violation of Title III. Smith rejected the Government's position that an "interception" occurs only when the contents of a wire communication are acquired contemporaneously with its transmission, finding that "contemporaneity" is required only for the interception of electronic communications.

7. While not afforded the level of protection afforded to communications in transit, stored communications, both oral or electronic, still receive significant protection from the Standards. See Part VIII of the Standards.

fact that it is transmitted to more than one recipient, and despite the lawful access of the provider to the contents of that communication.

Commentary to Standard 2-2.1(b)

These Standards protect a communication—no matter its type—only if the communication is "private" within the meaning of Standard 2-2.1(b). Title III, however, requires an expectation of privacy for oral communications, but not for wire and electronic ones. This difference in approach should not be construed to imply that the present Standards exclude from protection wire and electronic communications that, because of the technology by which they are transmitted, are more vulnerable to interception (e.g., wireless communications). Indeed, while the users of new communication technologies should be made aware of the extent to which their communications are vulnerable to interception, that vulnerability ought not be the sole factor in determining whether the user has a reasonable expectation of privacy. In particular, it should be clear that for purposes of these Standards, people who speak over conventional, cordless, cellular, and satellite telephones do so with a reasonable expectation of privacy, and their

9. Although the term "private communication" was not defined in the First or Second Edition of the Standards, each offered protection to wire and oral communications only when they were private. See, e.g., Standard 2-5.1 of the Second Edition of the Standards, which provided that an eavesdropping warrant should be required "for the overhearing or recording of wire or oral communications uttered in private without the consent of a party." See also Standard 2.9.2(f) of the Standards for Technologically Assisted Physical Surveillance, which defines "[a]n activity, condition or location [as] private when the place where it occurs or exists and other relevant considerations afford it a constitutionally protected reasonable expectation of privacy."

10. See 1 Carr, The Law of Electronic Surveillance (2000), at 3-6 ("Unlike the definition of oral communication in § 2510(2), the term wire communication does not include the element of an expectation of privacy on the part of the speakers") (footnote omitted). No doubt Title III protects a "wire communication" without explicitly incorporating a requirement of an expectation of privacy on the theory that such an expectation generally attaches to communications "made in whole or in part ... by the aid of wire, cable, or other like connection." 18 U.S.C. § 2510(1). See 18 U.S.C. § 2511(g) (excluding from the protections of Title III a variety of electronic and radio communications transmitted in a manner that makes them "readily accessible to the general public").

11. Congress recognized this in its treatment of cellular telephones, and, eventually, in its treatment of cordless ones as well. In the Electronic Communications Privacy Act, Congress extended the protections of Title III to communications over cellular telephones, even though courts had been unwilling to do so, see, e.g., Edwards v. State Farm Insurance, 833 F.2d 535 (5th Cir. 1987) (not unlawful for individual to overhear with radio scanner conversation over mobile telephone), and Congress was itself "aware that cellular
conversations are "private communication[s]" within the meaning of Standard 2-2.1(b).

In the case of face to face communications, Standard 2-2.1(b) takes a similar approach to Title III in defining a "private communication" as one "made under circumstances in which a reasonable expectation of privacy exists." See 18 U.S.C. § 2510(2) limiting an "oral communication" telephones were vulnerable to interception: 'cellular telephone calls can be intercepted by either sophisticated scanners designed for that purpose, or by regular radio scanners modified to intercept cellular calls. House Report [No. 647, 99th Cong., 2d Sess. at 20, Senate Report [No.99-541, 99th Cong., 2d Sess., reprinted in] 1986 U.S. Code Cong. & Admin. News at 3563." Shubert v. Metrophone, Inc., 898 F.2d 401, 405 (3d Cir. 1990). However, Congress did follow previous court rulings in concluding that the warrantless interception of the radio portion of cordless telephonic communications should not be prohibited, because such transmissions could easily be overheard by anyone using an AM radio within the general geographical area in which the cordless phone was operating. See Sen. Rep. No. 99-541, 99th Cong., 2d Sess., 1986 U.S. Code Cong. & Admin. News at 3563. See also United States v. Roach, 55 F.3d 1236 (6th Cir. 1995) (cordless phone conversations not "oral communications" because "oral communications" are those in which there is an expectation of privacy and cordless telephonic communications are broadcast over radio waves which anyone can overhear); In re Askin v. McNulty, 47 F.3d 100, 104 (4th Cir. 1995) (Fourth Amendment did not prohibit warrantless interception of cordless telephonic communication); United States v. Smith, 978 F.2d 171, 174 (5th Cir. 1992) ("The argument that Title III applies to cordless phone communications has been uniformly rejected by every court that has considered it"); but see United States v. Hall, 488 F.2d 193 (9th Cir. 1973) (holding that a communication between two cordless telephones was not protected under Title III, but stating in dicta that intercepting a communication between one cordless telephone and one regular telephone would constitute electronic surveillance).

In 1994, however, when it passed the Communications Assistance for Law Enforcement Act, Congress reversed this determination and extended Title III's protection to such communications, concluding that it was subjectively reasonable for a person to expect that a cordless telephonic communication was private, even though, objectively, the communication was vulnerable to interception. This change has been somewhat cynically described as "an example of political reality overwhelming technological reality: although cordless phone conversations are susceptible to random inadvertent interception, so many people now use them that the pressure to protect them legally became irresistible." Fishman and McKenna, Wiretapping and Eavesdropping (2d Ed. 2000), at 3-25. For another, less cynical view, see Dunlap v. County of Inyo, 121 F.3d 715, 1997 WL 414380 (9th Cir. 1998) (unpublished opinion) ("Cellular telephones and electronic mail are both technologies of questionable privacy, but we nonetheless reasonably expect privacy in our cell phone calls and email messages"). As the observation in Dunlap suggests, technology should not dictate social policy. As technology improves, it could be argued that no expectation of privacy is objectively reasonable (the first prong of Katz) since the public is on notice that every communication can be readily captured. This is a dangerous and unacceptable position—the fact that communications can be captured does not mean that it is unreasonable to expect that they will remain private.
to one "uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation." Determining when oral communications are private can be difficult. Clearly, two people speaking alone in a room have a reasonable expectation of privacy, and two prisoners speaking in a jail cell do not. If whether privacy attaches to a conversation in an open field or on a public street is a closer question, and such determinations are best made on a case by case basis, rather than in the black letter of a standard or in a statute. Among the relevant factors are not only where the conversation is taking place, but also what steps, if any, the persons engaged in that conversation take to maintain its confidentiality.

As with "wire communications," the Standards approach electronic communications somewhat differently than Title III does, but the extent of the protection each offers is, in the end, the same. Although the definition of an "electronic communication" set forth in 18 U.S.C. § 2510(12) does not (like that for an "oral communication") limit that term to a communication transmitted "by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation," 18 U.S.C. 2511(2)(g) provides that it is not unlawful for any person "to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public."

While Standard 2-2.1(b) generally leaves it to the case law to define what a reasonable expectation of privacy is, it does specify that such an expectation is not defeated by the existence of two specified circumstances. First, new technology easily permits communications

13. See, e.g., Matter of John Doe Trader Number One, 894 F.2d 240 (7th Cir. 1990) (because trader in foreign currency pit of mercantile exchange did not have reasonable expectation that conversations were private, they were not "oral communications").
14. See 1 Carr, The Law of Electronic Surveillance (2000), at 3-11 ("The speaker’s desire and location remain factors to be considered . . . , and like questions of intent generally, the issue of an expectation of privacy must be resolved by a consideration of all the facts and circumstances. Among these might be the content and purpose of the conversation, how it was conducted, and the speaker’s precautions against being overhead") (footnote omitted).
15. See also 18 U.S.C. § 2511 (2)(g)(ii), which provides that it is not unlawful to intercept any radio communications that are transmitted under any of a variety of circumstances that make the transmission generally accessible to the public, and 18 U.S.C. § 2510(16), which defines the term "readily accessible to the public" as that term applies to radio communications.
Electronic Surveillance of Private Communications

to be transmitted to many people at once. For example, an e-mail or a recorded telephone message can be sent to dozens, even hundreds or more, of different parties. The Standard's definition of a "private communication" makes clear that a communication that is otherwise private does not lose its privacy simply because it is transmitted by the service provider to more than one recipient. Second, while the public has become increasingly aware that a service provider can monitor e-mail and other electronic communications of its users, it has long been true that communication service providers of all kinds, including telephone companies, have had and used such capabilities, if only for purposes of quality control and to detect the unauthorized use and abuse of their services. While these Standards recognize that such access is appropriate under defined circumstances, the definition of a "private communication" makes clear that a user may have a reasonable expectation of privacy in a communication "despite the lawful access of the provider to the contents of that communication."17

(c) "Electronic surveillance" is the non-consensual interception of the contents of a private communication by use of a mechanical, electronic or other device. For purposes of this definition:

Commentary to Standard 2-2.1(c)

The term "electronic surveillance" was not defined in the First or Second Edition of the Standards. As a result, many individual Standards were complicated by making reference to "the overhearing or recording of wire or oral communications uttered in private without the consent of a party." See, e.g. Standards 2-1.1 and 2-5.1 of the Second Edition. The

16. See, e.g., Standard 2-8.1(a), authorizing a private electronic communication service provider "to acquire, use and disclose the contents of the private communications transmitted over or stored with its service for any lawful purpose," and Standard 2-8.1(b), authorizing a public electronic communication service provider "to acquire, use and disclose the contents of the private communications of its customers and other authorized and unauthorized users" for a more limited number of purposes, including, inter alia, "to the extent necessary to render the service, and to maintain and protect the availability, integrity and confidentiality of the system." Standard 2-8.1(b)(i).

17. Note, however, that Standard 2-5.1(b) authorizes a law enforcement officer to intercept the contents of the communications of an unauthorized user of a provider when "the provider reasonably determines that the communications threaten to disrupt the provider's service," and "when the provider consents to the interception." Under such circumstances, an expectation of privacy by the unauthorized user would be unreasonable.
definition of this term was added to the Third Edition in order to streamline the subsequent Standards regulating "electronic surveillance," thus making them easier to understand.

(i) the "contents" of a communication are any information concerning the substance, purport, or meaning of that communication;

**Commentary to Standard 2-2.1(c)(i)**

The definition of the "contents" of a communication is taken from 18 U.S.C. § 2510(8), which provides that "'contents', when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport or meaning of that communication." This definition excludes from the term "contents" the information obtained from a "pen register" or "trap and trace device," at least to the degree that those devices disclose only the numbers dialed to connect to a telephone, and not any alpha-numerical message communicated (for example, tones used for telephone banking) after the connection is made.

(ii) the contents of a private communication are "intercepted" when they are acquired contemporaneously with their transmission;

**Commentary to Standard 2-2.1(c)(ii)**

The definition of the term "intercepted" constitutes a reaffirmation that while the non-consensual acquisition of any private communication is a search governed by the Fourth Amendment, the additional limitations and regulations applicable to "electronic surveillance" should be applicable only to the acquisition of a communication while in transit. While some might argue that it is no less intrusive to

---

18. Previously, 18 U.S.C. 2510(8) defined the "contents" of a communication as "any information concerning the identity of the parties to such communication or the existence, substance, purport or meaning of that communication." As Judge Carr has noted "[t]he purpose of the deletion, according to the legislative history of the amendment, was to eliminate any ambiguity about the lawfulness of the use of pen registers. The amendment also sought to make clear the distinction between contents of a communication and transaction records." 1 Carr, *The Law of Electronic Surveillance* (2000), at 3-62.5 (footnotes omitted).

19. See Steve Jackson Games v. United States Secret Service, 36 F.3d 457 (5th Cir. 1994) (by seizing computer and acquiring e-mail which was stored in it and which was
acquire a private communication stored with a communication service provider, the judgment reflected in the Standards is to the contrary. Thus, the Standards embody both a subjective determination that a person’s sense of privacy is more undermined by the acquisition of a communication while it is in still in transit, and an objective determination that a communication in transit is less vulnerable to being heard or seen by others than one that has been recorded, however temporarily, by electronic or other means. Accordingly, the acquisition of communications stored with a service provider does not constitute electronic surveillance, and is governed by different Standards.

Because an interception occurs when the contents of a communication are contemporaneously “acquired,” once a communication is acquired, it is “intercepted,” even if the contents are not recorded, heard or read by any person, and even if it is not intelligible to the person who intercepts it. Thus, if a communication is in a foreign language or encrypted, it is intercepted when acquired, even if it is not translated or decrypted.

A communication is not intercepted, however, when its contents are not acquired (that is, not located and held) even momentarily, or, if they are momentarily retained, they are immediately, automatically and irrevocably deleted, since in either case, the contents never are, and never can be, recorded or heard or read by any person. Treating such a fleeting and imperceptible “acquisition” of a communication as an inter-
ception would accomplish nothing to protect privacy, but could arbitrarily and unnecessarily preclude the development and use of certain types of electronic surveillance equipment.

(iii) the contents of a communication are intercepted "non-consensually" when they are intercepted without the consent of at least one party to the communication; and

Commentary to Standard 2-2.1(c)(iii)

By defining "electronic surveillance" to exclude the interception of a communication with the consent of one of the parties, Standard 2-2.1(c) takes note of the longstanding constitutional rule that the consensual used only to acquire the contents of those electronic communications described in the court order, and (2) the contents of no other communication are held or, if held, are either never retained, or are immediately and permanently deleted without having been recorded, and without having been heard or read by any person. In a "packet-switched network," separating those communications covered by the court order from all others requires that "header" information be analyzed, but such information—such as the sender’s and recipient’s address—can be “acquired” because it is not content. When an applicant intends to use a "Carnivore"-type device—or, for that matter, any other device or technique raising unique privacy issues—the application should alert the judge to the its possible use and provide the court with sufficient information about how it functions to assure that its use is lawful. Note that Congress has recently required that such a report be made to the court when a law enforcement agency implements a pen register or trap and trace order “by installing and using its own . . . device on a packet-switched data network of a provider of electronic communication service to the public,” 18 U.S.C. 3123(a)(3), as added by USA PATRIOT Act, § 216, that is, by using what the legislative history refers to as a ""Carnivore'-like device." Congressional Record, October 25, 2001, S11007. In such a case, the agency must maintain a record (automatically, if possible) which identifies: (1) the officer or officers who installed or used the device; (2) the date and time it was installed and uninstalled, and the date, time, and duration of each time the device was used to obtain information; (3) “the configuration of the device at the time of its installation and any subsequent modification thereof;” and (4) any information collected by the device. 18 U.S.C. 3123(a)(3)(A). A report of this information must be made to the judge who issued the order within thirty days of the termination of the order. 18 U.S.C. 3123(a)(3)(B). The sunset provision applicable to most other electronic surveillance-related provisions of the USA Patriot Act is inapplicable to this provision.

22. To make an analogy: the unaided human eye does not perceive—that is, acquire—infrared light even though, technically, the light waves of that length and frequency pass through the eye’s lens. Acquisition, in short, requires access, possession or control.

23. Thus, the Standards reject the conclusions that courts have sometimes reached based upon the misguided premise that such a meaningless “acquisition” of a communication constitutes an “interception.” In People v. Bialostok, 80 N.Y.2d 738 (1993), for
recording of a communication does not implicate the Fourth Amendment, and reaffirms that, for purposes of the Standards, the requirements for a Fourth Amendment search, and the enhanced protections applicable to the non-consensual interception of private communications, should not be required when one of the parties consents to the interception. While the term “party” is not defined by the Standards, it should be clear that a party is a participant in the communication, and that a communications service provider may not, for purposes of this definition, “consent” to the interception of the communications of its authorized or unauthorized customers. Concerning the consensual interception of communications, see Standard 2-5.1.

Under federal law, “a person not acting under color of law [may] intercept a wire, oral or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.” 18 U.S.C. § 2511(2)(d). Some states permit a person not acting as an agent of law enforcement to intercept a communication with the consent of a party to the communication only in limited

instance, the New York Court of Appeals held that the use of a pen register device required an electronic surveillance order because the device, with modification, was capable of “acquiring” conversations, even if no communications were intercepted (that is, no information concerning the substance, purport, or meaning of that communication was acquired), and even if the modification that would permit such interceptions was never made. This logic led, in Bialostok and other cases, to the suppression of evidence obtained by subsequent court ordered electronic surveillance because the court orders were obtained, in part, on information obtained from use of the pen register. It also led to complex judicial attempts to draw an ultimately arbitrary line between pen register devices for which an electronic surveillance order was necessary and those for which one was not, based upon their susceptibility to misuse for interception. See People v. Kramer, 92 N.Y.2d 529 (1998). The Court of Appeals ultimately abandoned Bialostok, relying on the adoption (even before the Bialostock decision) of statutes governing the use of pen register devices, which required only an order based on reasonable suspicion, and which did not exclude from the definition of a “pen register” a device capable of being converted for use in acquiring conversations. See People v. Martello, 93 N.Y.2d 645 (1999). 24. United States v. White, 401 U.S. 745 (1971).

25. Before its amendment in 1986, § 2511(2)(d) also prohibited consent interceptions by a private party “for the purpose of committing any other injurious act.” Concerning the elimination of this language, see 1 Carr, The Law of Electronic Surveillance (2000), at 3-110-3-111.
circumstances, and other states entirely prohibit such a person from recording his or her own communications, or those of others, without the consent of all of the parties to the communication. The Standards take no position as to whether or when a private person not acting as an agent of law enforcement should be permitted to intercept a communication between other persons with the consent of only one of the parties to that communication.

(iv) a "mechanical, electronic or other device" means any device or apparatus which can be used to intercept the contents of a private communication other than any instrument, equipment or facility, furnished to or by the subscriber to or user of an electronic communication service which is installed and used in the ordinary course of the subscriber's business; or by an investigative or law enforcement officer in the ordinary course of the officer's duties.

Commentary to Standard 2-2.1(c)(iv)

The First and Second Editions of the Standards made reference to "the use of a mechanical, electronic, or any other device for overhearing or recording of wire or oral communications," see, e.g., Standard 2-2.1 of the Second Edition, without defining what such devices were. The definition of a "mechanical, electronic or other device" in the Third Edition is largely taken from 18 U.S.C. § 2510(5). The differences between this definition and that in § 2510(5) are stylistic only, and are not meant to give the term a different meaning under the Standards than it has under federal law.

The definition of a "mechanical, electronic or other device" includes an exception for "any instrument, equipment or facility, furnished to or by the subscriber to or user of an electronic communication service which is installed and used in the ordinary course of the subscriber's business." This exception is also contained in 18 U.S.C. § 2510(5), and has come to be known as the "business use" exception. It is meant to apply, for example, not only to a "regular extension phone being used in a normal way," but also to equipment companies' use to monitor

27. 1 Carr, The Law of Electronic Surveillance (2000), at 3-60 (footnote omitted). Some but not all courts considering the applicability of the exception to a regular extension
their employees' use of telephone and electronic communications services for purposes of quality control, or to prevent the use of such services for personal rather than business reasons.\textsuperscript{28} The employer may engage in such monitoring without notice only when it is justified by a valid business purpose.\textsuperscript{29} In applying this exception, the term "in the ordinary course of business" should be strictly construed, so that the exception does not swallow the rule.\textsuperscript{30} The exception for a device used "by an investigative or law enforcement officer in the ordinary course of the officer's duties," see also 8 U.S.C. § 2510(5)(a)(ii), should also be strictly construed for its intended purpose, and not to render the prohibition against warrantless electronic surveillance by law enforcement meaningless by permitting it whenever a law enforce-

---

\textsuperscript{28} Watkins v. L.M. Berry & Co., 704 F.2d 577 (11th Cir. 1983) (while it might be proper for employer to intercept an employee's calls in the ordinary course of business in order to deter employee's use of business line for personal calls, interception was proper only to determine whether call was personal, and any additional interception would be unwarranted). See also 1 Carr, \textit{The Law of Electronic Surveillance} (2000), at 3-6.2-3-6.3.

\textsuperscript{29} See Sanders v. Robert Bosch Corp., 38 F. 3d. 736, 741 (1994) ("In light of the Act's clear purpose of protecting individuals' privacy interests, the determination of whether the "use" made of a surveillance device falls within the ordinary course of business so as to satisfy section 2510(5)(a)(i) necessarily entails examination of whether such "use" was covert or open. Covert use of a surveillance device must be justified by a valid business purpose").

\textsuperscript{30} See 1 Carr, \textit{The Law of Electronic Surveillance} (2000), at 3-62.2 (noting that if the cases allow this exception to develop "the purpose of [Title III] to regulate secret eavesdropping could be substantially undone").
ment agency uses it routinely. Notice is generally necessary for the law enforcement exception.

Title III also includes an exception for a device "being used by a provider of wire or electronic communication service in the ordinary course of its business." 18 U.S.C. § 2510(5)(a)(ii). This exception is not included in Standard 2-2.1(c)(iv)'s definition of a "mechanical, electronic or other device," because Standard 2-8.1(b) more directly authorizes a public electronic communication service provider "to acquire, use and disclose the content of the private communications of its customers and other authorized and unauthorized users" for certain specified purposes, thus rendering this exception at best unnecessary, and at most, overly broad.

Subdivision (b) of 18 U.S.C. § 2510(5) also excludes from the term "a hearing aid or similar device being used to correct subnormal hearing to not better than normal." While Standard 2-2.1(c) contains no comparable exclusion, it was omitted because such language was deemed unnecessary, and not because the Standards meant to provide that "electronic surveillance" occurs when a person overhears a conversation using a device that does no more than make otherwise subnormal hearing normal.

31. "Congress most likely carved out an exception for law enforcement officials to make clear that the routine and almost universal recording of phone lines by police departments and prisons, as well as other law enforcement institutions, is exempt from the statute." Adams v. City of Battle Creek, 250 F.3d 980, 984 (2001), citing First v. Stark County Board of Commissioners, 234 F.3d 1268 (6th Cir. 2000), 2000 WL 1478389 (unpublished opinion). "As one court noted, 'Investigation is within the ordinary course of law enforcement, so if "ordinary" were read literally warrants would rarely if ever be required for electronic eavesdropping, which was surely not Congress's intent.'” 1 Carr, The Law of Electronic Surveillance (2000), at 3-62.3, quoting Amati v. City of Woodstock, 176 F.3d 952, 955 (7th Cir. 1999). Concerning the law enforcement exception, see generally, Carr, id., at 3-60-3-62.4 (2000).

32. In Adams v. City of Battle Creek, 250 F.3d 980, 984 (2001), the court noted that for purposes of the law enforcement exception, a device that intercepts communications is used in the "ordinary course of business" when that use is "(1) for a legitimate business purpose, (2) routine and (3) with notice." Id.

33. See also Standard 2-8.1(a), which permits an electronic communication service provider not offering its services to the public "to acquire, use and disclose the contents of the private communications transmitted over or stored with its service for any lawful purpose." And see 1 Carr, The Law of Electronic Surveillance (2000), at 3-70 (noting that 18 U.S.C. 2511(2)(a)(i) "expressly permits company employees to intercept communications when necessary to render service or protect the rights or property of the company,"
(d) "Minimization" is a good faith effort made to limit the interception of communications to those communications, or portions thereof, which are subject to interception pursuant to an electronic surveillance order.

Commentary to Standard 2-2.1(d)

The term "minimization" was not defined either in the previous editions of the Standards or in Title III. The definition must be read in conjunction with Standard 2-2.1(e), which explains when communications are "subject to interception." Standard 2-4.8(j) implements the minimization requirement by providing that an electronic surveillance order must contain "a directive that minimization of the intercepted communications be accomplished contemporaneously with their interception." Concerning the meaning of the minimization requirement, see the commentary to Standard 2-4.8(j). Concerning the minimization of communications after their interception, and the circumstances in which it is permitted, see Standard 2-4.9.

(e) A communication is "subject to interception" if it is intercepted during lawfully conducted electronic surveillance and:

(i) it is evidence of an offense which is an authorized subject of the electronic surveillance, or of another offense; and

(ii) the communication is not privileged under applicable state law.

Commentary to Standard 2-2.1(e)

A communication is "subject to interception" only during electronic surveillance that is lawfully conducted, that is, if it is conducted in the execution of a court order issued pursuant to Standard 2-4.1, or in an emergency situation without a warrant pursuant to Standard 2-5.2. The communication must either be evidence of an offense which is an authorized subject of the electronic surveillance, see Standard 2-4.8(e) (requiring that an electronic surveillance order must specify "the particular offense as to which electronic surveillance is approved"); or it

making unnecessary "the more convoluted authority contained in § 2510(5)(ii) and its exemption from the definition of intercepting device").

34. See also Standard 2-4.9, authorizing minimization after communications are intercepted when contemporaneous minimization "is not reasonably possible."
must be evidence "of another offense" when a communication relating to such other offense may be intercepted pursuant to Standard 2-4.5. Finally, to be "subject to interception," the communication may not be "privileged under applicable state law." Of course, communications otherwise privileged are not so if the communications relate to a crime which the parties to the communication have conspired or are conspiring to commit.

(f) "Law enforcement officer" means:
   (i) any officer of the United States or of a state or one of its political subdivisions who is empowered by law to conduct an investigation of, or to make an arrest for, a criminal offense, and includes any agent of such an officer, and
   (ii) any attorney authorized by law to prosecute or participate in the prosecution of such an offense.

Commentary to Standard 2-2.1(f):

This definition is adopted from 18 U.S.C. § 2510(7), which defines a "law enforcement officer" as (1) "any officer of the United States or of a State or political subdivision thereof, who is empowered by law to conduct investigations of or to make arrests for offenses enumerated in this chapter" and (2) "any attorney authorized by law to prosecute or participate in the prosecution of such offenses." Standard 2-4.8(c) requires that an order authorizing electronic surveillance contain "the identity of the agency employing the law enforcement officers authorized to intercept communications."

35. Concerning privileged communications, see Standard 2-4.12(a) (requiring a particularized showing of need for an order authorizing the interception of communications "over a facility or in a place primarily used by professionals whose communications are privileged under state law, or in a place used primarily for habitation by a husband and wife"); and Standard 2-4.12(b) (providing that when an otherwise privileged communication is intercepted, it should not lose its privileged character).

36. "If ... a claim of privilege is invalidated because the parties (i.e., attorney and client, or husband and wife) were coconspirators, no special obligation to minimize [the interception of their communications] arises simply as the result of the relationship, and otherwise privileged communications can be intercepted without violating the minimization requirement." 1 Carr, The Law of Electronic Surveillance (2000), at 5-35, citing United States v. Harrelson, 754 F.2d 1153, 1166-69 (5th Cir. 1985).
By including an "agent" of a law enforcement officer within this definition, subdivision (i) permits experts outside of law enforcement who are fluent in a foreign language or proficient in a code to intercept communications in that language or code and minimize them contemporaneously with their interception, or to minimize after their interception communications which could not be contemporaneously minimized. See Standard 2-4.9.\textsuperscript{37} In order for such an expert to be an "agent" of a law enforcement the expert must engage in this activity under the supervision of the officer. This definition also permits the cross-designation of law enforcement officers who are not necessarily "empowered by law to conduct an investigation of, or to make an arrest for" the criminal offense which is the subject of an electronic surveillance order. This process allows the cross-designated officers to participate in the execution of the order as agents and under the supervision of law enforcement officers who are so empowered. See the commentary to Standard 2-4.1(c).

\textbf{(g) An "electronic communication service provider" is a person or entity which, in the ordinary course of business, routinely provides a service allowing its users to send or receive private communications, and a "public electronic communication service provider" is one who offers such a service to the public.}

\textit{Commentary to Standard 2-2.1(g)}

An "electronic communication service provider" may transmit private communications and may store them for their intended recipients. The Standards govern when law enforcement may intercept communications transmitted by or through such services, see Part IV of the Standards, and when it may acquire the contents of communications stored

\textsuperscript{37} While 18 U.S.C. § 2510(7) does not include in its definition of "law enforcement officer" an "agent of such an officer," 18 U.S.C. § 2518(5) provides that "[a]n interception . . . may be conducted in whole or in part by Governmental personnel, or by an individual operating under a contract with the Government, acting under the supervision of an investigative or law enforcement officer authorized to conduct the interception." According to the legislative history of the 1986 amendment that added this language to § 2518(5), the purpose of the amendment was much broader than permitting outside experts to intercept communications in a foreign language or code. Rather, Congress meant to "free professional agents from the 'relatively routine activity of monitoring interceptions.'" 1 Carr, \textit{The Law of Electronic Surveillance} (2000), at 5-5, quoting House Report No. 99-647, 99th Cong., 2d Sess., 1986 U.S. Code Cong. & Admin. News 3555.
with such services, see Standard 2-8.2. The Standards also govern the right of providers to acquire, use and disclose the contents of the communications sent or received by the users of their services. See Standard 2-8.1. As defined, the term “electronic communication service provider” includes not only those entities that provide a service permitting its customers and users to transmit non-aural electronic communications like e-mail, but also telephone companies that transmit the human voice. In a definition added to Title III by ECPA, 18 U.S.C. § 2510(15) similarly defines an “electronic communication service” as “any service which provides to users thereof the ability to send or receive wire or electronic communications.” Within the meaning of Standard 2-2.1(f), entities like the Post Office and Federal Express are not electronic communication service providers when they transmit written communications, rather than “the human voice or of any signs, signals, writing, images, sounds, data or intelligence of any nature, by wire, radio wave, or other technological means.”

This Standard distinguishes a “public electronic communication service provider” from a private one because Standard 2-8.1(b) carefully circumscribes the right of public providers to acquire, use and disclose the contents of the communications of those who use their service. However, Standard 2-8.1(a) permits private providers to do so “for any lawful purpose.” Federal law makes a similar distinction, by regulating when “a person or entity providing an electronic communication service to the public” may divulge “the contents of a communication while in electronic storage by that service,” 18 U.S.C. § 2702, but making no comparable provision concerning private providers. Another provision, 18 U.S.C. § 2511, which governs when a wire or electronic communication service may “intercept, disclose or use” a communication, also includes a limitation for “a provider of wire communication service to the public,” not applicable to private providers. Concerning the reason for this distinction in treatment, see the commentary to Standard 2-8.1(a).

This definition limits an “electronic communication service provider” to one who furnishes such a service “routinely,” and “in the ordinary course of business.” To fall within this definition, the provider need not be in the business of providing communication service, but need only provide that service routinely, and in the ordinary course of whatever its business may be.

Federal law regulates the disclosure of electronic communications stored not only by an “electronic communication service provider,” but also by a “remote computing service,” which is defined as “the provision
to the public of computer storage or processing service by means of an electronic communications system." 18 U.S.C. § 2711(2). While no comparable definition appears in Standard 2-2.1, the Standards are nonetheless applicable to a remote computing service whenever such a service acts as an "electronic communication service provider" by enabling its customers to transmit electronic communications to the service and by storing those communications with the service.

38. An "electronic communications system" is defined by 18 U.S.C. § 2510(15) as "any wire, radio, electromagnetic, photooptical or photelectronic facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications."
PART III.
GENERAL PRINCIPLES

Standard 2-3.1. General principles

The standards that follow incorporate and implement these general principles:

Commentary to Standard 2-3.1

The First and Second Editions of the Standards contained a much shorter set of "General Principles" for electronic surveillance of private communications. A more detailed list was included in this Edition in order to set forth, in black letter, all of the value determinations incorporated and implemented in the Standards that follow. Many of the principles newly set forth in Standard 2-3.1 were, in any case, implicit in the First and Second Edition of the Standards; others resolve policy questions raised by new technology, including the advent and growth of electronic communications. Standard 2-3.1 follows the format used for the statement of General Principles set forth in Standard 2-9.1 of the Standards of Technologically-Assisted Physical Surveillance (Section B of these Standards).

The General Principles are divided into three areas: (a) the need to protect private communications; (b) the need to allow regulated electronic surveillance by law enforcement; and (c) applying for and executing an electronic surveillance order.

(a) The need to protect private communications.

(i) Intrusion on private communications by the government. The security of private communications from arbitrary intrusion by governmental officials is a basic necessity for the maintenance of a free society. Accordingly, law enforcement's authority to conduct electronic surveillance should be strictly regulated.

39. See Standard 2-1.1 of the Second Edition, which contains only stylistic and conforming changes from Standard 1.1 of the First Edition. Subdivision (a) of Standard 2-1.1 is a statement of the objectives of the Second Edition; subdivisions (b) and (c) include statements of general principles. The Third Edition states its objectives in an earlier and separate Standard, Standard 2-1.1.
Commentary to Standard 2-3.1(a)(i)

As the Supreme Court first observed in Wolf v. Colorado, and re-affirmed in Berger v. New York, "[t]he security of one's privacy against arbitrary intrusion by the police—which is at the core of the Fourth Amendment—is basic to a free society."40 In United States v. Katz, the Supreme Court declared that a person who makes a telephone call from a public telephone booth should be able to "assume that the words he utters into the mouthpiece will not be broadcast to the world," and that "[t]o read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication."41 In Berger, the Court also took note of the warning of Chief Justice Warren, concurring in Lopez v. United States, that "the fantastic advances in the field of electronic communication constitute a great danger to the privacy of the individual," and that "indiscriminate use of such devices in law enforcement raises grave constitutional questions under the Fourth and Fifth Amendments . . . ."42 Indeed, in Berger, the Court warned that "[f]ew threats to liberty exist which are greater than that posed by the use of eavesdropping devices." 388 U.S. at 63.43

Similarly concerned about the effect of electronic surveillance on privacy, the First Edition of the Standards announced that law enforcement's use of electronic surveillance should be "[s]ubject to strict statutory limitations."44 Indeed, the First Edition "began with the judgment that the interest of privacy in our society demands that all private and public use of electronic surveillance techniques to overhear private communications be prohibited," and that "[o]nly the most compelling showing of need can justify an exception to this general principle."45 Since the First Edition

43. When it enacted Title III, Congress made a similar finding: "The tremendous scientific and technological developments that have taken place in the last century have made possible today the widespread use and abuse of electronic surveillance techniques... No longer is it possible, in short, for each man to retreat into his home and be left alone. Every spoken word relating to each man's personal, marital, religious, political, or commercial concerns can be intercepted by an unseen auditor and turned against the speaker to the auditor's advantage." Senate Report No. 1097, 90th Cong., 2d Sess., 1968 U.S. Code Cong. & Admin. News, 2122, 2159.
44. Standard 1.1(c) of the First Edition. See also Standard 2-1.1 (c) of the Second Edition.
was issued, technological advances have continued to produce ever more sophisticated devices for communicating privately, and the proliferation, convenience and popularity of these devices have increased our reliance on them. At the same time, however, the use of these devices has made the private communications which they transmit and receive more susceptible to interception, enhancing the need for comprehensive regulation of electronic surveillance by law enforcement.

(ii) Intrusion on private communications by others. Because technology renders private communications vulnerable to interception by all persons, electronic surveillance by those outside law enforcement should also be strictly regulated.

Commentary to Standard 2-3.1(a)(ii)

This statement of principle recognizes that the technology that permits law enforcement to conduct electronic surveillance is also available to those outside of law enforcement. The danger of private electronic surveillance has also increased with technological developments in electronic communications and electronic surveillance. As the 1986 Senate Report for the Electronic Communications Privacy Act pointed out, since Title III became law, "tremendous advances in telecommunications and computer technologies have carried with them comparable technological advances in surveillance devices and techniques." The Report warns not only of the danger that "overzealous law enforcement agencies" may engage in illegal electronic surveillance, but also that "[e]lectronic hardware making it possible for . . . industrial spies and private parties to intercept the personal or proprietary communications of others are readily available on the market today."46 Thus the Third Edition of the Standards, like the first two, prohibits the interception of private communications by private parties, and also strictly regulates the disclosure of private communications by public electronic communication service providers to others.

(iii) Protecting stored communications. When technologically transmitted private communications are stored by an electronic

Electronic Surveillance of Private Communications

Commentary to Standard 2-3.1(a)(iii)

Providers of electronic communication services usually store communications incidental to their transmission to their intended recipients. This storage creates, albeit temporarily, a record of what would otherwise be ephemeral, and thus reduces somewhat the expectation that a third party will never hear or see the communication. Nonetheless, a party to such a stored communication has a reasonable expectation of privacy, and the reasonableness of that expectation of privacy is greatest when the communication is stored for only a brief period of time, and when it is truly incidental to its transmission. See the commentary to Standard 2-8.2(a)(ii) and (iii). Because the privacy of a communication can be compromised through access to the content stored with the provider, the law should also regulate access to the contents of such stored private communications.

(iv) Providing the same level of protection for all forms of communication. Private communications should be afforded the same level of protection whether they are spoken in person or transmitted by technological means, and if by technological means, whether or not the communications include the human voice.

Commentary to Standard 2-3.1(a)(iv)

When Congress enacted the Electronic Communications Privacy Act in 1986, it recognized the omnipresence and importance in our society of new forms of electronic communications which do not involve transmission of the human voice. Concluding that electronic communications deserved an expectation of privacy like that associated with communications including the human voice, and reacting to the concern "that current legal protections for electronic mail [were] 'weak, ambiguous, or not existent,' and that electronic mail remain[ed] legally as well as technically vulnerable to unauthorized surveillance,"47 Congress extended

many of the protections of Title III to electronic communications. There were, however, three omissions. First, while only the Attorney General and a limited number of Justice Department officials may apply for a warrant authorizing the interception of wire and oral communications, "[a]ny attorney for the Government (as that term is defined for purposes of the Federal Rules of Criminal Procedure)" may apply for a warrant authorizing the interception of electronic communications. Second, although an eavesdropping warrant authorizing the interception of wire and oral communications may be issued in connection with an investigation of a long but limited list of crimes, Congress provided that a federal warrant authorizing the interception of electronic communications may be issued in connection with an investigation of "any Federal felony." Third, Title III includes within it provisions for suppression of
Electronic surveillance evidence which has been unlawfully intercepted, a remedy the Supreme Court has made clear applies not only to constitutional violations, but to significant statutory ones as well, but there is no statutory remedy for the unlawful interception of electronic communications, and thus suppression is available only when the violation of law is constitutional in nature.

If a justification existed in 1986 for treating aural and electronic communications differently, it was because electronic communications were then used primarily by governments, businesses and universities. Congress thus may have viewed electronic communications as business records that deserve a lesser expectation of privacy. This rationale, however, relies on a vision of impersonal communications between large organizations, and fails to take into account the privacy interest of the individual members or employees of those organizations. It also fails to take into account the citizens, customers and clients of those large organizations, whose communications with these bodies may reveal much about their personal affairs, including but not limited to their

interception of wire and oral communications may be issued. Those crimes are "murder, kidnapping, gambling, robbery, bribery, extortion, or dealing in narcotic drugs, marijuana or other dangerous drugs, or other crimes dangerous to life, limb, or property, and punishable by imprisonment for more than one year." 18 U.S.C. 2516(2).

51. 18 U.S.C. 2515 provides that the contents of any wire and oral communications, and any evidence derived from those contents, may not be received in evidence at trial "if the disclosure of that information would be in violation of this chapter," and 18 U.S.C. 2518(10)(a) provides for suppression "of the contents of any intercepted wire or oral communication, or evidence derived therefrom, on the grounds that "(i) the communication was unlawfully intercepted; (ii) the order of authorization or approval under which it was intercepted is insufficient on its face; or (iii) the interception was not made in conformity with the order of authorization or approval."

52. In United States v. Giordano, 416 U.S. 505, 527 (1974), the Supreme Court concluded that "the words 'unlawfully intercepted' [in 18 U.S.C. 2510(a)(1)] are themselves not limited to constitutional violations, and we think Congress intended to require suppression where there is a failure to satisfy any of those statutory requirements that directly and substantially implement the congressional intention to limit the use of intercept procedures to those situations clearly calling for the employment of this extraordinary investigative device."

53. The legislative history to ECPA offers no rationale for this difference in treatment, and states only that it was adopted "as the result of discussions with the Justice Department." Senate Report No. 99-541, 99th Cong., 2d Sess., 1986 U.S. Code Cong. & Admin. News 3555, 3577. Among the important policies of Title III is the one that limits electronic surveillance to use as a last resort, a policy Congress implemented by requiring in 18 U.S.C. § 2518(1)(c) that an application for an electronic surveillance order demonstrate that "other investigative procedures have been tried and failed or . . . reasonably appear to be unlikely to succeed if tried or to be too dangerous." The Supreme Court has
Electronic Surveillance of Private Communications

2-3.1(a)(iv)

financial condition, the purchases they are making or contemplating, their travel plans, and their intellectual and recreational interests. In any case, this rationale has largely been rendered obsolete by the exploding use of electronic communications by individuals for entirely private purposes. Parents and their children, friends and relatives scattered across the country and abroad, and those who are not related and have met only on-line, routinely communicate by fax, e-mail, and other forms of electronic communication.

Increasingly, individuals use electronic communications interchangeably with aural ones, trading the value of hearing the human voice for the convenience and savings, and sometimes the anonymity, attendant to communicating electronically.\(^{54}\) Moreover, the once clear distinction between electronic and voice communications is blurring. For example, a person may now choose to transmit to an e-mail box a communication that is entirely text, entirely voice, or a combination of the two, and by using a speech recognition program a person may create text by talking into a computer’s microphone, and the text may then be transmitted as ordinary e-mail. Given these developments, there is no reason why a spoken message dictated as an audio attachment to e-mail should be treated differently from e-mail which includes the same message but is conveyed entirely electronically,\(^{55}\) and there is no reason why a message dictated to speech recognition software should be treated differently from a message that originates in and remains human speech.\(^{56}\) In sum, there is no justification for giving greater protection to a communication which includes the human voice

---

\(^{54}\) Congress has recognized as much. See the Senate Report to the Electronic Communications Privacy Act of 1986, which observes that “American citizens and American businesses are using these new forms of [electronic communications] technology in lieu of, or side-by-side with, first class mail and common carrier telephone services.” Senate Report No. 99-541, 99th Cong., 2d Sess. 1986 U.S. Code Cong. & Admin. News 3555, 3559.

\(^{55}\) Indeed, when the human voice is digitized for transmission, the zeroes and ones with which it is composed are the same zeroes and ones with which electronic communications are created.

\(^{56}\) See Senate Report No. 99-541, 99th Cong., 2d Sess. 1986 U.S. Code Cong. & Admin. News 2555, 2570 (“[C]omputer-generated or otherwise artificial voices are not included in [the definition of ‘aural transfer’] and thus will not be part of a ‘wire communication’”). When the law treats such aural and non-aural communications differently, the distinctions are not only arbitrary, they are also difficult to apply and enforce. For example, a law enforcement officer who obtains authorization for the surveillance of electronic
than to one which is purely "electronic" but is otherwise identical in content. Thus, whether the communications sought are aural or non-aural, the Standards limit applicants for orders authorizing their interception to the same group of officials, see Standard 2-4.1(b), limit the offenses for which electronic surveillance may be authorized to the same list of crimes, see Standard 2-4.4, and provide the same constitutional and statutory grounds for their suppression. See Standard 2-6.2.

(b) The need to allow regulated electronic surveillance by law enforcement.

(i) Need for electronic surveillance. Because the interception of private communications can be an effective tool for the investigation and prosecution of criminal activity, law enforcement agencies should, in appropriate cases and under appropriate regulation, have the legal authority and the technological means to conduct electronic surveillance, and to use the communications thus lawfully obtained, and evidence derived therefrom, in criminal and related civil actions.

Commentary to Standard 2-3.1(b)(i)

Although the commentary to the 1968 Standards observed that "[o]nly the most compelling showing of need can justify" the overhearing of private communications, it also concluded that "there is a compelling social need to enforce the penal law in the area of organized crime" and "a clear and present law enforcement need . . . to employ these techniques of investigation in this and related areas."57 Although the Supreme Court once expressed some doubt concerning the efficacy of eavesdropping as a tool for the investigation and prosecution of organized crime,58 since

communications may intercept an e-mail only to learn after opening it that its interception is not authorized because it contains the human voice.

57. First Edition, General Commentary at 96. For the factual basis of these conclusions, see id., pp. 48–95. When it enacted Title III, Congress found that "[v]ictims, complainants, or witnesses are unwilling to testify because of apathy, fear or self-interest, and the top figures in the rackets are protected by layers of insulation and direct participation in criminal acts. Information received from paid informants is often unreliable, and a stern code of discipline inhibits the development of informants against organized criminals. In short, intercepting the communications of organized criminals is the only method of learning about their activities." Senate Report No. 1097, 90th Cong., 2d Sess. 1968 U.S. Code Cong. & Admin. News 2112, 2159.

58. Berger v. New York, 388 U.S. 41, 60 (1967) ("It is said with fervor that electronic eavesdropping is a most important technique of law enforcement and that outlawing it will severely cripple crime prevention. . . . However, we have found no empirical statis-
then the extraordinary success of this technique has made clear that court-ordered electronic surveillance can achieve extraordinary results not otherwise attainable. In 1986, the President’s Commission on Organized Crime noted that “[i]n the last four years, the leadership in 17 of 24 La Cosa Nostra families has been indicted or convicted,” and credited much of the success to the effectiveness of electronic surveillance. Since the Report was issued, electronic surveillance has continued to play an important role in the prosecution of the criminal activities of Cosa Nostra and other organized crime groups.
(ii) **Balancing competing needs.** A proper balancing of privacy and law enforcement interests requires that electronic surveillance by law enforcement agencies be permitted only when:

(A) the objectives of an investigation are not likely attainable by alternative investigatory methods, and

(B) the intrusion is justified by the importance and likelihood of achieving those objectives.

**Commentary to Standard 2-3.1(b)(ii)**

Having recognized, on the one hand, that maintenance of a free society requires the strict regulation of electronic surveillance and, on the other, that it can be an effective law enforcement tool, the general principles attempt to strike an appropriate balance between these competing interests. In any particular case, two factors must be considered: the necessity of the electronic surveillance to the objectives of the investigation, and the importance of those objectives and the likelihood of achieving them.

In Title III, and in the Standards (past and present), the necessity of the electronic surveillance is not merely a factor for a court or applicant to consider—demonstrating that the objectives of the investigation cannot be achieved by other means is an absolute requirement for issuance of an electronic surveillance order. The Supreme Court has said that Congress imposed the 'necessity' requirement "to assure that [electronic surveillance] is not resorted to in situations where traditional investigative techniques would suffice to expose the crime," and that Congress "evinced the clear intent to make doubly sure that the statutory authority be used with restraint" and that wiretapping and bugging "were not to be routinely employed as the initial step in criminal investigation."

While satisfying the necessity requirement is thus critical, it is not the only appropriate factor to consider before electronic surveillance is initiated. Even in a case in which electronic surveillance is the only way in

---

See also United States v. Hurley, 63 F. 3d 1 (1st Cir. 1995) (defendant convicted of laundered hundreds of millions of dollars on behalf of international drug cartels).

62. See Standard 2-4.3(c) (requiring that application establish "that for purposes of achieving the authorized objectives of the electronic surveillance as described in the application, other investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous."). See also 18 U.S.C. § 2518(1)(c).


which the objectives of the investigation may be achieved, those objectives may not be sufficiently significant to justify the resulting intrusion on privacy, particularly if the likelihood of achieving those objectives is not great. Whether the necessity requirement has been satisfied is a decision that must be made by the court when asked to issue an electronic surveillance order, but whether the intrusion of the electronic surveillance is justified by the importance and likelihood of achieving its objectives is a determination best left to the discretion of the applicant, who is politically accountable for his or her electronic surveillance policy.65

(iii) Constitutional requirements. Except in emergency circumstances, electronic surveillance should be permitted only when authorized by a prior judicial order, which should be issued and executed in compliance with the Fourth Amendment requirements of probable cause, particularity, notice, and reasonableness.

Commentary to Standard 2-3.1(b)(iii)

In 1967, in Katz v. United States, the Supreme Court held that the non-consensual interception of private communications constitutes a search, and that the propriety of that search, like any other, is governed by the Fourth Amendment.66 Earlier that same year, in Berger v. New York, the Court set out the constitutional requirements for an electronic surveillance order.67 Fundamental to Katz and Berger was the principle that, in the absence of exigent circumstances, an intrusion on private communications requires prior court authorization. Indeed, in Katz, the Court rejected the argument that a seizure of a telephonic communication was proper because, although it was not authorized by court order, it was nonetheless reasonable. Finding it "apparent that the agents in this case

65. See Standard 2-3.1(c)(i). An applicant for an electronic surveillance order must set forth facts demonstrating the necessity of the electronic surveillance, Standard 2-4.2(a)(xi), and the judge to whom the application is made must determine whether the showing made by the applicant satisfies the necessity requirement. See Standard 2-4.6(b). While Standard 2-4.6 invites the judge to exercise his or her "sound discretion" in determining whether to issue the order, the Standards intentionally do not direct the judge to consider whether the importance of the investigation outweighs the intrusiveness of the electronic surveillance. Concerning the political accountability of an applicant, see the commentary to Standard 2-3.1(c)(i)(A).
acted with restraint," the Court nonetheless condemned the seizure based upon "the inescapable fact . . . that this restraint was imposed by the agents themselves, not by a judicial officer."68

The requirements for an electronic surveillance order set forth in Berger include: (1) probable cause that a particular offense has been, is being, or is about to be committed, and that evidence of that crime may be obtained by the eavesdropping sought; (2) particularization of those persons whose communications are to be intercepted, the place in or facility over which those communications are occurring, and of the type of communications to be seized; (3) reasonable limitations on the duration and breadth of the authorized eavesdropping; (4) a return to the judge who issues the electronic surveillance order; and (5) notice to the subjects of the surveillance.69 Each one of these requirements has been incorporated into the Third Edition of the Standards, as, of course, they were in the previous two editions and in Title III.

Standards 2-4.2(a)(x), 2-4.3(a) and (b), and 2-4.6(b) set forth the probable cause showings that an applicant must make, and that a judge must find have been made, before an electronic surveillance order may be issued. Standard 2-4.2(iv), (v), (vii) and (viii) and 2-4.8(d), (e), (f) and (g) implement the particularization requirements of person, crime, communication and facility or place.70 Standards 2-4.8(j) and (k) establish the limitations of reasonableness by requiring that the interception of non-pertinent and privileged communications be minimized and by restrict-

68. Katz v. United States, 389 U.S. 347, 356 (1967). "‘Over and over again this Court has emphasized that the mandate of the [Fourth] Amendment requires adherence to judicial processes’ . . . and that searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment—subject only to a few specially established and well-delineated exceptions.” Id., at 357. (Citations and footnotes omitted). See also Berger v. New York, 388 U.S. 41, 55 (1967) (noting that the Fourth Amendment requires for eavesdropping that “a neutral and detached authority be interposed between the police and the public”).

69. Berger v. New York, 388 U.S. 41, 54–60 (1967). Concerning the return to the court and inventory notice to the eavesdropping subjects as constitutional requirements, see United States v. Donovan, 429 U.S. 413, 429, n. 19 (1977). Berger also speaks of a required showing of exigency to justify the lack of prior notice to the subject of the search. Berger v. New York, 388 U.S. at 60. However, the Supreme Court made clear in Katz v. United States, 389 U.S. 347, 355, n. 16 (1967), that when electronic surveillance is lawfully authorized, advanced notice is unnecessary because it would defeat the purpose of the surveillance. See United States v. Agrusa, 541 F.2d 690, 698 (8th Cir. 1976).

70. Note, however, that there are exceptional circumstances in which the facility or place need not be specified. See Standard 2-4.10.
Electronic Surveillance of Private Communications

2-3.1(b)(iv) Non-constitutional requirements. When law enforcement acquires a private communication non-consensually, the intrusion on privacy is greater if the contents are acquired contemporaneously with the transmission of the communication. Consequently, the use of electronic surveillance by law enforcement should be subjected to requirements beyond those mandated by the Fourth Amendment.

Commentary to Standard 2-3.1(b)(iv)

In addition to provisions designed to ensure that electronic surveillance orders are obtained and executed in compliance with the requirements of the Fourth Amendment, the Standards give recognition to the particular intrusiveness of electronic surveillance through requirements that regulate and restrict its use that are not constitutionally mandated. These requirements include: restricting who may apply for an electronic surveillance order [see Standard 2-3.1(c)(1) and Standard 2-4.1(b)]; permitting court authorized electronic surveillance only as a last resort [see
Standard 2-3.1(c)(i)(C), Standard 2-4.2(a)(xi), Standard 2-4.3(c), and Standard 2-4.6(b); limiting the offenses which may be the subject of an electronic surveillance order [see Standard 2-4.4]; and requiring that the execution of an electronic surveillance order be supervised by an attorney [see Standard 2-3.1(c)(ii)(A) and Standard 2-4.2(iii)] and overseen by the judge issuing the order [see Standard 2-3.2(c)(iii)].

(v) Regulating law enforcement's access to stored communications. Because the privacy interests in private communications stored incidental to their transmission are also significant, the law should also strictly regulate law enforcement's authority to acquire and use the contents of such stored private communications.

Commentary to Standard 2-3.1(b)(v)

In his prescient dissent in Olmstead v. United States,1 Justice Brandeis drew an analogy between written and telephonic communications, expressing the view that, "[t]here is, in essence, no difference between the sealed letter and the private telephone message." While both are, in fact, private communications the interception of which constitutes a search for which probable cause must be shown,72 an important distinction exists in the manner of both their transmission and interception. A letter is, of course, first written and then mailed to its intended recipient, while the words of a telephone conversation are transmitted to the person to whom they are directed at the same time they are uttered. Similarly, when a letter is intercepted and its contents read, the interception occurs only after the letter is written and sent, but a telephonic communication is intercepted at the same time it is transmitted to and heard by the other party to the communication. Because the interception is contemporaneous with the transmission, electronic surveillance is a greater intrusion for which greater protection is appropriately given by the Standards and by Title III. See Standard 2-3.1(b)(iv).

However, new technology has created a hybrid between letters and telephone calls: electronic communications that are created and then

---

1. 277 U.S. 438, 475 (1927).
stored incidental to their transmission. For example, electronic mail is sent to an electronic communication service provider and stored with the provider until and often after it is retrieved by the recipient. The Electronic Communications Privacy Act protects messages in electronic storage, which it defines in part as "any temporary, intermediate storage of [an] . . . . electronic communication incidental to the electronic transmission thereof." 18 U.S.C. 2510 (17)(A). Like ECPA, the Standards do not afford to the acquisition of stored private communications the same level of protection given to communications intercepted simultaneously with their transmission. While the lesser level of protection is justified by the transformation of what is otherwise ephemeral into something more concrete, electronic storage of at least some private communications is a necessary part of their transmission, and storage of such communications for at least some period of time is a necessary part of their reception by the parties to whom they are transmitted. For this reason, stored communications are deserving of significant protection.

(c) Applying for and executing an electronic surveillance order.

(i) Establishing the necessity for electronic surveillance. Electronic surveillance is an especially intrusive means of investigation. Accordingly, a judicial order authorizing a law enforcement officer to conduct electronic surveillance should be issued only when:

(A) the application for the order has been approved by a politically accountable prosecutor with the authority to establish and maintain a uniform electronic surveillance policy within the affected jurisdiction, or by a high ranking subordinate expressly authorized to exercise this responsibility;

Commentary to Standard 2-3.1(c)(i)(A)

Standard 2-3.1(c)(A) limits those officials who may apply for electronic surveillance orders. The purpose of the limitation is to give applicant authority to those who may develop and execute a uniform electronic surveillance policy within the relevant federal, state or local jurisdiction,

73. Indeed, telephonic communications, like electronic ones, can be stored by telephone companies for later access by their intended recipients. Telephone companies now provide a service by which callers can leave voice messages, which, because they include the human voice, would constitute "stored" wire (as opposed to electronic) communications.

74. Concerning the protection afforded to stored communications, see Part VIII of the Standards.
2-3.1(c)(i)(A)  

*Electronic Surveillance of Private Communications*

and to hold them accountable for the policies they develop and the manner in which they carry out those policies. The general principle set forth in this Standard is implemented by Standard 2-4.1, which specifies what federal, state and local officials may apply for an electronic surveillance order,75 and by Standard 2-6.2, which mandates suppression of communications intercepted pursuant to an order issued upon the application of an unauthorized official.

By requiring that the applicant be a "prosecutor," this Standard rejects the decision some jurisdictions have made to allow high ranking officials who are not prosecutors to apply for electronic surveillance orders.76 While high ranking officials who are not prosecutors may be politically accountable, they lack the prosecutorial knowledge and experience necessary to make the judgements by which to develop and implement an electronic surveillance policy.

Just as the "politically accountable" prosecutor must be an attorney, so must any "high ranking subordinate" to whom the prosecutor could delegate applicant authority. By restricting applicants to "high ranking subordinates" of state and local prosecutors, the Standard does not mean to preclude delegation of applicant authority in a small office in which the principal prosecuting attorney may have only a few, or even just one, assistant.

(B) the applicant believes that the intrusion is justified by the importance and likelihood of achieving the objectives of the electronic surveillance; and

*Commentary to Standard 2-3.1(c)(i)(B)*

In carrying out the electronic surveillance policies they develop, applicants should do more than simply determine if the legal require-

75. See also Standard 2-5.2(a), which specifies what federal, state and local officials may authorize warrantless electronic surveillance in an emergency situation.

76. See 1 Carr, *The Law of Electronic Surveillance* (2000) at 4-23 ("Some states allow other officials to authorize applications for electronic surveillance orders," including the Chairman of the New Jersey State Commission on Investigation, the Deputy Attorney General in charge of the New York State Organized Crime Task Force, and the Governors of Florida and Wyoming, and the courts have held that the designation of these officials does not violate Title III). Note, however, that the Deputy Attorney General in charge of the New York State Organized Crime Task Force is an attorney. See People v. Vespucci, 75 N.Y.2d 434 (1990) (statutory designation of Director of New York State Organized Crime Task Force as applicant for eavesdropping warrant consistent with federal law limiting applicant to "principal prosecuting attorney" of state).
ments for electronic surveillance have been met. Among those added responsibilities is determining whether, although legally permissible, electronic surveillance is justified when balancing the degree of the intrusion with the importance and likelihood of achieving the objectives of the investigation. How this balance should be struck depends, of course, both on the seriousness of the criminal conduct under investigation and the weight of the affected privacy interest. Preventing or providing evidence of the commission of a crime of substantial violence could warrant interception of private communications even if they were occurring in a bedroom. On the other hand, while a bookmaking operation unrelated to an organized criminal group may represent no great threat to society, neither is there any great privacy interest in communications occurring over a telephone line installed in a wireroom used for virtually nothing else but the promotion of gambling. If, however, electronic surveillance could uncover evidence of a small bookmaking operation unconnected to other organized criminal activity, but only by intercepting communications over a telephone that many persons who were not a target of the investigation used for innocent purposes, the applicant might decide that the benefits of the surveillance were outweighed by the costs.

(C) the judge issuing the order approves the objectives of the electronic surveillance and finds that for purposes of achieving those objectives, other investigative procedures have been tried and have failed, or reasonably appear to be unlikely to succeed if tried or to be too dangerous.

Commentary to Standard 2-3.1(c)(i)(C)

This general principle gives further specificity to the requirement set forth in Standard 2-3.1(b)(ii) that electronic surveillance should only be permitted when "the objectives of an investigation are not likely attainable by alternative investigatory methods" (see the commentary to that Standard) and makes clear that the obligation for enforcing this "necessity" requirement rests with the judge. This requirement of "necessity" is implemented by Standard 2-4.3(c), which requires that the application for an electronic surveillance order make this showing; by Standard 2-4.2(xi), which requires that the application include the "material facts relevant to the applicant and necessary for the [judge] to determine" whether this showing has been made; and by Standard 2-4.6(b), which permits the judge to grant the application only if the judge determines that this showing has been made.
Note that this statement of general principle not only requires the judge to determine whether or not the applicant has demonstrated the requisite necessity, but also requires the judge to approve the objectives of the investigation. This provision in the General Principles is implemented by Standard 2-4.8(l), which requires that an electronic surveillance order contain "a directive that the interception of communications shall terminate upon the authorized objectives of the electronic surveillance, as those objectives . . . are approved by the court." See also Standard 2-4.8(m). This requirement is new to the Third Edition of the Standards. By imposing it, this Standard does not invite the judge to determine whether an investigation is "worthy" of electronic surveillance, for example, by balancing the intrusiveness of the electronic surveillance against the importance of the objectives. That determination is left to the applicant. See Standard 2-3.1(c)(i)(B). Rather, the judge must determine whether the objectives are reasonable given the probable cause showings made in the application. In other words, if the application demonstrates probable cause to believe that crimes which are lawfully the subject of an electronic surveillance order have been, are being, or about to be committed, and that evidence of those crimes can be obtained by the electronic surveillance sought, the appropriate inquiry for the judge is: are the objectives of the investigation directed toward the prosecution of those crimes and are those objectives reasonably obtainable?

(ii) Employing the expertise required. Officers executing an electronic surveillance order often must make complex legal determinations. Accordingly,

(A) the execution of such an order should be supervised by an attorney authorized to investigate and prosecute the crimes which are the subject of the order, and

Commentary to Standard 2-3.1(c)(ii)(A)

When the police obtain a conventional search warrant, they may generally apply for and execute the warrant without prosecutorial involvement. The situation is fundamentally different, however, for electronic surveillance. Not only must a high ranking prosecutorial official authorize the application for an electronic surveillance order (see Standard 2-3.1(c)(i)(A)), but a prosecuting attorney must be responsible for supervising its execution. Over the days, weeks or months during which an
Electronic surveillance order is executed, the officers executing the order are called upon to make thousands of decisions: to intercept some communications because they are relevant to the crime which is the subject of the order, and not to intercept others because they are not relevant to that crime; to intercept a communication because it is evidence of a crime not named in the order, or to cease the interception of a communication because it appears to be privileged. The expertise of a prosecuting attorney is necessary in supervising these sometimes difficult determinations. Moreover, a prosecuting attorney can better decide whether and when the objectives of the investigation have been achieved, since prosecutors are routinely called upon to consider what a jury may find sufficient evidence to establish guilt beyond a reasonable doubt, while police officers are more accustomed to determining if the lesser threshold of probable cause has been attained.

The attorneys who supervise the surveillance may review these determinations by examining the logs of the interceptions and copies or transcripts of portions of the intercepted communications, and by meeting with the intercepting officers and discussing the issues which have arisen. Armed with the information they thus receive, the attorneys may not only review the appropriateness of any particular execution decision, but may also issue oral and written instructions, clarifying their interpretation of what the order does and does not permit. Although the previous editions of the Standards, like Title III, did not specifically mandate on-going supervision of the electronic surveillance by a prosecuting attorney, they assumed that such supervision would result from the requirement that the applicant not only make the application for the original court order authorizing the surveillance, but also for any extensions and amendments of that order.77 The Third Edition of the Standards takes realistic note of the fact that, for a variety of practical reasons, the execution of an electronic surveillance order may be far removed from the official who authorized the application for the order.78 The Standards also reflect a grave concern for even the possibility that after an applicant obtained an electronic surveillance order,

77. "The role envisioned by the prosecutor [who authorizes an application for an electronic surveillance order] under the Standards serves several other policies as well. The prosecutor's legal expertise should ensure compliance with statutory requirements, thereby protecting both privacy from unnecessary intrusion and surveillance evidence from suppression." Introduction to the Second Edition at 2-9.

78. The most obvious example of such a situation is when the applicant for an electronic surveillance order is the Attorney General of the United States, and the order is
no prosecuting attorney would participate in its execution until it became necessary to seek an additional court order. Thus, Standard 2-3.1(c)(ii)(A) states that "the execution of . . . an [electronic surveillance] order should be supervised by an attorney authorized to investigate and prosecute the crimes which are the subject of the order," and Standard 2.4-8 makes a particular prosecuting attorney responsible and accountable for the execution of the order by requiring [in subdivision (b)] that the order identify the prosecuting attorney who will supervise the order's execution, and [in subdivision (m)] by explicitly requiring that the identified attorney "or another prosecuting attorney acting on his or her behalf" exercise that supervision. Standard 2-4.8(m).

(B) communications should be intercepted pursuant to the order by law enforcement officers who have been trained in the law and techniques of electronic surveillance, and who understand the terms and conditions of the order.

Commentary to Standard 2-3.1(c)(ii)(B)

This statement of general principle is also new to the Standards. It is implemented in part by subdivisions (iv) and (vi) of Standard 2-7.1, which require that law enforcement agencies provide such training to their officers. Inevitably, executing officers will be called upon to make on-the-spot determinations concerning the interception of communications between parties not named in the electronic surveillance order, those of questionable relevance to the subject matter of the order, those that are cryptic or in a foreign language, or those that may fall under some legal privilege. While supervision of the execution of an electronic surveillance order by a prosecuting attorney is mandated by the previous provision, that supervision does not supplant the need for executing officers who are sufficiently familiar with the basics of the law and techniques of electronic surveillance to determine which communications and which portions of communications to intercept, and how to intercept them. Indeed, a trained officer is better equipped than an untrained one to recognize problems beyond his or her expertise and more likely to take them to the supervising prosecutor for resolution.

executed in a federal district far removed from Washington, D.C. Geography, however, is not the only problem. Even the District Attorney's office of a large county may be too large to make personal supervision by the District Attorney practical.
Thus, electronic surveillance orders are best executed by officers who have such training, and law enforcement agencies whose officers are regularly involved in electronic surveillance should routinely offer such training to those officers, including programs to refresh and update their knowledge, since changes and developments in the law can be expected. If the exigencies of an investigation require the participation of officers who have not previously had such training, time and care should be taken to provide those officers with at least a general familiarity with the legal issues they are likely to confront, and the prosecuting attorney supervising the execution of the order should take particular note of their work.

Even an officer who is familiar with the law and techniques of electronic surveillance cannot effectively execute an electronic surveillance order without understanding its terms and conditions. That understanding is best gained when each of the executing officers reads the order and the underlying application in their entirety, and when the order is further explained by the supervising prosecutor, who should instruct the intercepting officers, as Standard 2-7.1(a)(vi) requires, "concerning the crime for which electronic surveillance has been authorized, the objectives of the electronic surveillance, the parties whose communications may be intercepted, the types of communications which may be intercepted, and the obligation to minimize the interception of communications which are not otherwise subject to interception." The supervising prosecutor's instructions should also include any particular minimization instructions the judge has issued, or any the prosecutor is imposing which are not contained in the order. Execution may be limited, for example, to particular days of the week, particular times of the day, or to other external factors (for example, observation at the premises of a named party), and an officer unfamiliar with those limitations may inadvertently engage in illegal electronic surveillance.

(iii) Judicial monitoring of on-going electronic surveillance.

Because an electronic surveillance order is usually executed over an extended period of time, the judge who issues such an order can and should ensure that it is executed appropriately.

Commentary to Standard 2-3.1(c)(iii)

When the police employ conventional investigative techniques requiring a search warrant, except for the ministerial receipt of the
return on the warrant, judicial participation generally begins and ends with the judge's decision to grant or deny the warrant. For electronic surveillance, however, the issuing judge has responsibilities that continue throughout the execution of the order. Under the first two editions of the Standards, judicial oversight was possible when the judge issuing an electronic surveillance order required the submission of progress reports concerning the ongoing surveillance (see the commentary to Standard 2-4.8(m)) and by the requirement that application be made to the judge for amendments and extensions of the original order.\textsuperscript{79} Standard 2-3.1(c)(iii) goes further than the previous editions—and further than Title III—by explicitly providing that "the judge who issues such an order can and should ensure that it is executed appropriately." The ability of the judge to carry out this responsibility is enhanced by Standard 2-4.8(m), which requires the supervising prosecutor to submit progress reports, unless the authorized period of surveillance is ten days or less.\textsuperscript{80} This provision and others ensure that the judge will be notified of important developments in the execution of the order. See, e.g., Standard 2-4.8(m)(ii) (judge must be notified in progress report of interception of communications relating to offenses other than those specified in order); Standard 2-4.9(b) (judge must be notified of minimization of communications after their interception).

While it is both necessary and desirable for attorneys who are authorized to investigate and prosecute the crimes which are the subject of an electronic surveillance order to supervise its execution, such supervision is not a substitute for the oversight of the neutral magistrate who issued the order. Given the extended period of surveillance usually authorized, and given that if judicial review does not occur during the electronic surveillance, it may not occur until long after it is over, the lack of contemporaneous judicial monitoring can have undesirable results. For those whose communications are intercepted, overly broad surveillance of their

\textsuperscript{79} See, e.g., in the Second Edition, Standards 2.5.9 (concerning extensions) and 2-5.6 (concerning amendments approving the interception of a communication relating to an offense not the subject of the order).

\textsuperscript{80} Standard 2-4.8(m)(i) requires that reports include "information reasonably adequate to permit the judge to review whether the order is being executed in a manner which minimizes the interception of communications not otherwise subject to interception, and whether continued interception of the communications pursuant to the order is necessary to achieve the objectives of the electronic surveillance, as those objectives are set forth in the application pursuant to Standard 2-4.2(vi) and approved by the court pursuant to Standard 2-4.8(l).
communications may result without effective remedy thereafter. For law enforcement, the investigation may proceed without knowledge that communications which have been seized are subject to later suppression, at which time not only those communications, but also their fruits, will be lost. Indeed, for law enforcement, contemporaneous judicial monitoring of the electronic surveillance may have an added benefit. When suppression and appellate courts review the propriety of the execution of an electronic surveillance order, they will know that the judge who issued the order was in a position to supervise its execution,\textsuperscript{81} and they may defer to determinations made by the issuing judge concerning close minimization questions.\textsuperscript{82}

(iv) Creating a reliable record. To maximize the reliability of evidence obtained through the interception of private communications, a record of the contents of the communications thus intercepted should, whenever technologically possible, be made and preserved in a manner designed to protect its integrity.

\textit{Commentary to Standard 2-3.1(c)(iv)}

This general principle is implemented by Standard 2-4.14, which contains various requirements concerning the authenticity of the records of intercepted communications. See the commentary to subdivision (b) of that Standard. See also subdivisions (iii) and (viii) of Standard 2-7.1, which, respectively, require that the administrative regulations of law enforcement agencies "set out the manner in which the techniques [of electronic surveillance] must be used to assure authenticity," and "restrict the transcription of, custody of, and access to, overheard or recorded communications by agents."

\textsuperscript{81} See, e.g., United States v. Kahn, 415 U.S. 143, 154 (1974) ("... the order limited the length of any possible interception to 15 days, while requiring status report as to the progress of the wiretap to be submitted to the District Judge every five days, so that any possible abuses might be quickly discovered and halted"); United States v. Vento, 533 N.2d 838, 861-2) (3d Cir. 1976) (failure to include minimization provision in eavesdropping warrant as required by Title III did not require suppression, where despite the absence of the minimization provision, the agents were instructed to carry out minimization procedures, they in fact did so, and progress reports were submitted to the court which permitted it to exercise close supervision).

Ensuring accountability. To further ensure the accountability of law enforcement officials and officers who participate in electronic surveillance, law enforcement agencies should:

Commentary to Standard 2-3.1(c)(v)

This Standard is derived from Standard 2-9.1 of the Third Edition, which sets forth general principles for accountability and control for the use of technologically-assisted physical surveillance, and the commentary to that Standard is, to some degree, relevant here as well. In emphasizing the need to ensure accountability, the commentary to Standard 2-9.1 notes that in some situations, the use of electronically-assisted physical surveillance “may never become known to its subjects,” and observes that some forms of such surveillance are “not memorialized through a warrant and its accompanying paperwork.” Neither of these concerns are applicable to electronic surveillance of private communications, which requires that the subjects of the surveillance receive notice that it has occurred even if no prosecution results (see Standard 2-4.15) and for which a court order, application and other paperwork is necessary. Nonetheless, the need for accountability remains, not only for applicants for electronic surveillance orders, but also for the law enforcement agencies whose officers execute those orders.

(A) promulgate administrative rules to ensure that the information necessary for such accountability exists;

Commentary to Standard 2-3.1(c)(v)(A)

As the following examples illustrate, officials who are authorized applicants for electronic surveillance orders should have administrative rules requiring the gathering and maintenance of a variety of kinds of informational records. First, keeping a complete record of all previous electronic surveillance applications is necessary, so that when the applicant authorizes the making of an application to intercept the communications of particular persons, over particular facilities, and at a particular

---

place, the applicant can—as the Standards and Title III require—furnish the judge to whom the application is made with accurate information concerning previous applications for electronic surveillance of those persons, facilities and places. See Standard 2-4.2(a)(xii). Second, the creation and review of records concerning the applications made by a particular applicant, and the results of the electronic surveillance conducted under the applicant’s authority, can assure that the applicant has the information necessary to evaluate the consistency of the applicant’s electronic surveillance policy and the effectiveness of the authorized surveillance. In particular, when the law permits high ranking subordinates of the principal prosecuting attorney to exercise applicant authority, such records can reveal when and under what circumstances those subordinates applied for electronic surveillance orders, and whether their applications reflect the electronic surveillance policy of their principal. Third, administrative rules can require the maintenance of records concerning the training in the law and techniques of electronic surveillance the applicant has furnished to the attorneys who supervise the execution of electronic surveillance orders and to those law enforcement agencies whose officers have or will execute electronic surveillance orders for which the applicant is responsible.

The administrative regulations appropriate for law enforcement agencies whose officers execute electronic surveillance orders are set forth in Standard 2-7.1. Many of these regulations will provide the information necessary to hold the agencies and their officers accountable for the electronic surveillance in which they participate. See, e.g., subdivision (a)(i), which provides for regulations limiting the number of officers in the agency authorized to conduct electronic surveillance; and subdivision (a)(v), which provides for regulations requiring the close supervision of officers authorized to conduct electronic surveillance. In addition, pursuant to subdivision (iv) of Standard 2-7.1, which provides for regulations requiring that officers who execute electronic surveillance orders first be trained in the law and techniques of electronic surveillance, law enforcement agencies should maintain their own records documenting which of their officers have received electronic surveillance training and when. Pursuant to subdivision (vii) of Standard 2-7.1, administrative rules can also mandate comprehensive record keeping concerning the custody, maintenance and use of electronic surveillance equipment, so that the agency can assure that the equipment is used only for the purposes and in the manner for which it was designed, and only when authorized by law.
Electronic Surveillance of Private Communications

(B) be subject to the exclusionary sanction in appropriate circumstances;

Commentary to Standard 2-3.1(c)(v)(B)

This statement of principle is implemented by Standard 2-6.2, which sets forth the circumstances in which the suppression of intercepted communications, and evidence derived from such communications, should be suppressed. When communications are suppressed for trivial and inadvertent mistakes having no effect on privacy, the suppression remedy can appear arbitrary and unpredictable, diminishing both accountability and respect for the law.\(^85\) However, when applied to constitutional errors and significant statutory ones, suppression is an effective means for ensuring accountability and deterring unlawful conduct. Indeed, the severity of its consequences—and the public forum in which it is imposed—provides a powerful incentive to those who participate in electronic surveillance to take care that it is properly conducted in accordance with the law. The availability of the exclusionary sanction encourages the applicant—usually the principal prosecuting attorney ultimately responsible for the success or failure of any prosecution resulting from the electronic surveillance—to ensure that the application for and execution of an electronic surveillance order complies with constitutional and legal requirements. The law enforcement officers who execute such an order must work closely with the prosecuting attorney who supervises its execution, and that prosecuting attorney is likely to be responsible for the resulting prosecution and answerable to the applicant. If some or all of the evidence obtained through the electronic surveillance is suppressed, the supervising attorney will likely be called upon to defend the application of the order and its execution, and the officers will no doubt learn of its suppression and of the reasons for it. Thus, they, too, will have a powerful incentive to comply with the mandates of the law and of the court order, and, if mistakes are made, will learn of them and how to correct them.

85. "Particularly when law enforcement officers have acted in objective good faith or their transgressions are minor, the magnitude of the benefit conferred on... guilty defendants offends basic concepts of the criminal justice systems... Indiscriminate application of the exclusionary rule, therefore, may well 'generate disrespect for the law and the administration of justice.'" United States v. Leon, 468 U.S. 897, 907–08 (1984).
(C) promulgate internal regulations concerning the manner in which electronic surveillance is authorized and conducted;

**Commentary to Standard 2-3.1(c)(v)(C)**

An official authorized by law to be an applicant for electronic surveillance orders should promulgate internal regulations concerning the application process. Applications should be reviewed to insure that they comply with all legal requirements, and that review should be conducted by persons thoroughly familiar with the facts of the investigation and with the law of electronic surveillance. Familiarity with the facts of the investigation is required to ensure that the judge to whom the application is made receives all the material facts necessary in determining whether the application should issue. Familiarity with the law is required in order to ensure that the application is legally sufficient, that all those who should be the subject of the order are named as such, and that the form of the order otherwise complies with the law. The process of review is sufficiently complicated to make the development of a checklist useful and not merely ministerial.

Beyond determining whether an electronic surveillance order is legally sufficient and proper, the applicant must also decide whether "the intrusion is justified by the importance and likelihood of achieving the objectives of the electronic surveillance." Standard 2-3.1(b)(ii)(A). In that connection, the applicant should also play his or her intended role of developing and maintaining a uniform electronic surveillance policy within the applicable jurisdiction. For both of these purposes, internal regulations can be useful by requiring the applicant to articulate an electronic surveillance policy, and by developing a mechanism for reviewing each application in light of that policy. In formulating that policy, the regulations should include, as set forth in Standard 2-7.1(a)(ii), a "specification of the circumstances under which [electronic surveillance] should be used, giving preference to those which invade privacy least."

The applicant's internal regulations can also do much to effectuate the proper execution of electronic surveillance orders. In addition to "set[ting] out the manner in which [electronic surveillance] must be used to assure authenticity," such regulations could also usefully address the process of minimization. General rules should be established, for example, for the length of time an intercepting officer has to determine whether a communication is relevant or not to the crime which is the subject of the electronic surveillance (see the commentary...
to Standard 2-4.8(j)) and a protocol could be established for conducting minimization after communications are intercepted, to be used cases in which such after-the-fact minimization is appropriate. See Standard 2-4.9. Similarly, categories of situations might be developed in which it would be necessary to bring a minimization issue to the attention of the supervising attorney, or of the judge who issued the order. Finally, internal regulations could establish a uniform method and format for creating a record of the minimization process—what officer was conducting the minimization, when intercepting and recording of a communication began and ended, who the parties were, and a summary of what they discussed. Such uniformity would be of particular importance when—as frequently happens—more than one law enforcement agency takes part in executing an order. While minimization inherently requires the exercise of individual discretion, and the appropriate method and degree of minimization necessarily varies from case to case, internal regulations can provide a baseline for the procedure to be usually followed, from which departures could be justified on a case by case basis.

While subject to the supervision and regulations of the applicant, law enforcement agencies whose officers execute electronic surveillance could usefully establish their own regulations concerning the execution of electronic surveillance orders. In some situations—for example, when state police officers execute an electronic surveillance order obtained by an applicant who is the district attorney in a small county—the agency may have much more experience with the process than the applicant, and the agency's own internal procedures may necessarily be the primary source of guidance. Thus, law enforcement agencies without applicant status, but with substantial electronic surveillance experience, could profitably develop their own rules for minimization, similar to those described above. In some cases, the law enforcement agency, rather than the applicant, will become the custodian of the records made of intercepted communications, and the custody and protection of those records would also be an appropriate subject for uniform rules.

(D) periodically review the scope and effectiveness of the electronic surveillance conducted; and

Commentary to Standard 2-3.1(c)(v)(D)

Best positioned to gauge the effectiveness of the electronic surveillance he or she (and his or her subordinates) has authorized, an appli-
Electronic Surveillance of Private Communications

2-3.1(c)(v)(E)

cant ought periodically to take stock of the number and kind of orders obtained, their duration and intrusiveness, the crimes for which the surveillance was authorized, and the cost and success of the surveillance. By gathering and reviewing this information, an applicant can determine whether the electronic surveillance policy in effect over a particular period was followed. Moreover, the applicant can determine whether the policy was effective in: (1) achieving the objectives of the investigations in which it was sought; (2) balancing the adverse effect on privacy with the gain in public safety; and (3) ensuring that the costs of using this technique (e.g., manpower, equipment, facilities and other expenses) proved reasonable and sensible. The policy, or its implementation, could then be amended as needed. Perhaps too many resources were devoted to electronic surveillance in matters that were ultimately of little importance, or perhaps opportunities to achieve significant results were lost because electronic surveillance was terminated too early, or not attempted at all.

Because electronic surveillance is so expensive to conduct—both in terms of personnel and expenditures for equipment and communications services—law enforcement agencies who devote much of their time to cases involving electronic surveillance must also be sure that their investment is cost effective. While not charged, as an applicant is, with establishing and carrying out an electronic surveillance policy within his or her jurisdiction, a law enforcement agency must decide for itself whether participating in electronic surveillance in a particular case is consistent with its own goals and available resources. Alternatively, it may, based on its own experience with electronic surveillance, be able to convince an applicant that electronic surveillance the applicant is reluctant to undertake would be worthwhile. While such determinations could be made on an ad hoc basis, a thorough documentation and review of the agency’s history would be far more useful.

(E) maintain and make available to the public general information about the type or types of electronic surveillance conducted, and the frequency of their use.

Commentary to Standard 2-3.1(c)(v)(E)

This statement of principal is implemented by Standard 2-4.17, which requires applicants and judges to provide detailed reports to “an appropriate agency” concerning the applications made for electronic
surveillance orders and the prosecutions brought with the evidence obtained in executing them. This provision is substantially similar to 18 U.S.C. § 2519, which results each year in the issuance of a report by the Administrative Office of the United States Courts, which lists the requisite information for the federal government and the states, jurisdiction by jurisdiction, thus permitting interested parties and the general public to see what use specific applicants have made of electronic surveillance and with what results. Despite the fact that these reports necessarily take the form of a dry recitation of statistics, they often generate media coverage concerning the amount, kind, expense and results of electronic surveillance in various jurisdictions, and are sometimes cited and analyzed in more scholarly work on the subject. These reports also permit the identification of those officials who have the authority to apply for electronic surveillance orders but choose not to do so, and those who apply for such orders in connection with the investigation of some designated offenses but not others.
PART IV.
COURT-ORDERED ELECTRONIC SURVEILLANCE

Standard 2-4.1. Order authorizing electronic surveillance; authorized application

(a) Except in an emergency situation, law enforcement officers should be permitted to conduct electronic surveillance only when authorized by a judicial order of the highest court of general trial jurisdiction, or a court authorized to hear appeals from that court.

Commentary to Standard 2-4.1(a)

This Standard is derived from Standard 2-5.1 of the Second Edition of the Standards. In addition to stylistic changes, it includes a few other minor modifications. First, for the purpose of clarity, Standard 2-4.1(a) includes a reference to the exception to the rule announced in this Standard, which permits electronic surveillance without a court order “in an emergency situation.” While the prior editions of the Standards also included such an exception, no reference to it was made in the predecessors to this particular provision.

Second, in specifying what judge should be permitted to issue an electronic surveillance order, Standard 2-4.1(a) includes not only a judge of “the highest court of general trial jurisdiction,” as its predecessor provisions did, but also of “a court authorized to hear appeals from that court.” The addition was made because in some states, the geographical limitations of a court of general trial jurisdiction may be quite small—encompassing only one or a few counties. In such circumstances, an applicant seeking authority to conduct electronic surveillance in two or more locations or over two or more facilities may be required to obtain authority to do so from more than one judge, even though the locations and facilities are relatively close to one other. Difficulties may ensue from having orders issued in the same case by more than one judge—for example, conflicting minimization instructions, overlapping notice requirements, and duplication of paperwork (since each judge must be notified of the progress made in the electronic surveillance the other(s) have authorized. While these problems are not insurmountable, they are also unnecessary, since there is no principled reason to preclude a judge of an appellate court,
(b) An application for such an order should be permitted:
   
   (i) in the case of an order directed to a federal law enforcement officer, only when authorized by the Attorney General of the United States, or, when specifically permitted by Congress, by any other high ranking subordinate whom the Attorney General specially designates to authorize such applications, and who is either a presidential appointee or a person with appropriate expertise in applications for electronic surveillance orders; and

   (ii) in the case of an order directed to a state or local law enforcement officer, only when authorized by the principal prosecuting attorney of the state or local government, or by a high ranking subordinate, when specifically permitted by state law and when specially designated by the principal prosecuting attorney to authorize such an application.

Commentary to Standard 2-4.1(b)

This Standard implements the general principle announced in Standard 2-3.1(c)(i)(A) that the application for an electronic surveillance order should be made only when it “has been approved by a politically accountable prosecutor with the authority to establish and maintain a uniform electronic surveillance policy within the affected jurisdiction, or by a high ranking subordinate expressly authorized to exercise this responsibility.” Standard 2-1.1(c) of the Second Edition of the Standards (like its predecessor in the First) stated that “. . . the Attorney General of the United States, the principal prosecuting attorney of a state or local government, or law enforcement attorneys or officers acting under his or her direction should be permitted to use electronic

86. Appellate court judges are permitted to issue electronic surveillance orders in the District of Columbia, Florida, Kansas, Minnesota, New York and Ohio, and state supreme court justices are permitted to issue orders in Arizona, Colorado, Florida, Kansas, Minnesota, Nevada and North Dakota. See Carr, The Law of Electronic Surveillance (2000), at 4-110–4-111. While the Standards do not authorize the issuance of electronic surveillance orders by a supreme court justice of a state if a lower appellate court is authorized to hear appeals from the highest court of general trial jurisdiction, courts have upheld state statutes that include such provisions. Id. at 411.
surveillance techniques," and Standard 2-5.1 of the Second Edition (like its predecessor) provided that an application for an order authorizing such techniques must be "authorized by the appropriate prosecuting officer as described in Standard 2-1.1(c)."

Placing a strict limitation on those officials who may authorize applications for electronic surveillance has from the outset been a central requirement for the interception of wire and oral communications under Title III. See 18 U.S.C. § 2516. As the Supreme Court has noted, limiting those who can authorize applications for an electronic surveillance order "centralizes in a publicly responsible official subject to the political process the formulation of law enforcement policy on the use of law enforcement techniques. Centralization will avoid the possibility that divergent practices might develop. Should abuses occur, the lines of responsibility lead to an identifiable person. This provision in itself should go a long way toward guaranteeing that no abuses will happen."87 While Title III "provides for a wider dispersal of authority among state officers to approve wiretap applications and leaves the matter up to state law, . . . it is apparent that Congress desired to centralize and limit this authority where it was feasible to do so, a desire easily implemented in the federal establishment . . . ."88

When Congress enacted the Electronic Communications Privacy Act in 1986, it did not limit applicants for federal orders authorizing the interception of electronic communications (that is, those not including the human voice) to this list of officials, but instead permitted an application for such an order to be made by "[a]ny attorney for the Government." 18 U.S.C. § 2516(3).89 For the reasons set forth in the commentary to Standard 2-3.1(a)(iv), the Standards reject the lesser protection thus afforded to electronic communications under Title III, and place the same limitation on applicants for orders authorizing the interception of all forms of private communications.

The list of those officials of the Justice Department who may authorize a federal application for an order permitting the interception of

89. Rule 54(c) of the Federal Rules of Criminal Procedure, in relevant part, defines "[a]ttorney for the government" as "the Attorney General, an authorized assistant of the Attorney General, a United States Attorney, [or] an authorized assistant of a United States Attorney."
wire or oral communications has repeatedly been amended. While accepting the need to permit a number of federal officials in the Justice Department to exercise this authority, the present Standard does not express that approval by mimicking the list in Title III, since that approach would make the Standards outdated, or in need of reconsideration, each time Congress added a new title to the list. Instead, the Standards speak generically, with language that offers some guidance as to what kind of officials should appropriately be included. Permitting a "presidential appointee" to be an applicant directly assures political accountability. Permitting high level officials “with appropriate expertise in applications for electronic surveillance orders” to exercise applicant authority allows responsibility to be given to someone knowledgeable and experienced in the area, who is answerable to an official who is politically accountable.

For electronic surveillance at the state and local level, Standard 2-4.1(b) authorizes as an applicant not only the principle prosecuting officer of the state or local government, but also “a high ranking subordinate, when specifically permitted by state law and when specially designated by the principal prosecuting attorney to authorize such an application." While no comparable language appears in Title III, the legislative history of Title III does include the statement that "[t]he issue of delegation by [the principle prosecuting attorney] would be a question of State law," Senate Report No. 1097, 90th Cong., 2d Sess., 1968 U.S. Code Cong. & Admin. News., at 2187, and courts have relied upon this statement in permitting subordinates of the "principal prosecuting attorney" at the state and local level to apply for an electronic surveillance order.

(c) A law enforcement officer should be permitted to conduct court-ordered electronic surveillance only when that officer is empowered by law to conduct an investigation of, or to make an arrest for, the particular offense as to which electronic surveillance is approved.

90. Originally the list was limited to "[t]he Attorney General, or any Assistant Attorney General specially designated by the Attorney General." The list now includes "[t]he Attorney General, Deputy Attorney General, Associate Attorney General or any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General or acting Deputy Assistant Attorney General in the Criminal Division specially designated by the Attorney General." 18 U.S.C. § 2516(1).

91. 18 U.S.C. § 2516(2) permits a state to give applicant authority to "[t]he principal prosecuting attorney of [the] State, or the principal prosecuting attorney of any political subdivision thereof."

92. See statutes and cases collected in Carr, Electronic Surveillance (2000), 4-25--4-26.
Electronic Surveillance of Private Communications

Commentary to Standard 2-4.1(c)

Standard 2-2.1(f) defines "law enforcement officer" as "any officer of the United States or of a state or one of its political subdivisions who is empowered by law to conduct an investigation of, or to make an arrest for, a criminal offense . . . ." Subdivision (c) of Standard 2-4.1 further specifies that, in order to be permitted to execute an electronic surveillance order, a law enforcement officer should have such power with respect to the particular offense which the judge has approved as the subject of the order. This provision parallels Standard 2-3.1(c)(ii), which states that "the execution of [an electronic surveillance] order should be supervised by an attorney authorized to investigate and prosecute the crimes which are the subject of the order." This provision is not meant to preclude a law enforcement officer who does not have such power from being cross-designated as an officer of another agency having authority to investigate or make an arrest for the crime. Thus, for example, consistent with this Standard, a state or local police officer may be cross-designated as a federal agent in order to take part in the execution of a federal electronic surveillance order, and a federal agent may be cross-designated as a state or local officer, in order to take part in the execution of a state order. Such a cross-designation should not, however, be a mere formality; a cross-designated officer must act on behalf and under the supervision of his or her superiors in the agency to which he or she is temporarily placed.

Standard 2-4.2. Application; form; contents; additional facts

(a) An application for an order authorizing the use of electronic surveillance should be made in writing upon an oath or affirmation and state:

   (i) the identity of the prosecuting official authorizing the application pursuant to Standard 2-4.1(b);

Commentary to Standard 2-4.2(a)(i)

This provision is identical to Standard 2-5.3(a) of the Second Edition, but for the explanatory reference to Standard 2-4.1(b).

93 See 1 Carr, The Law of Electronic Surveillance (2000), at 5-5 ("The agency specified in the order may use personnel from other law enforcement agencies as monitors while executing the surveillance order. In a federal surveillance, overhearing by cooperating state officers is not improper") (footnotes omitted).
(ii) the identity of the prosecuting attorney making the application;

Commentary to Standard 2-4.2(a)(ii)

The equivalent language in Standard 2-5.3(b) of the Second Edition is "the identity of the law enforcement officer making the application." The change emphasizes the need for the involvement of a prosecutor throughout the process of drafting and making an application for and executing an electronic surveillance order. The "prosecuting attorney" referred to here need not be the applicant who authorizes the application, and need not (but usually will be) the prosecuting attorney who will supervise its execution.

(iii) the identity of the prosecuting attorney who will supervise the execution of the order;

Commentary to Standard 2-4.2(a)(iii)

The previous editions of the Standards contain no comparable requirement that an individual be identified in the application as the person responsible for supervising the execution of the order. This provision was added to implement Standard 2-3.1(c), which requires supervision of the execution of the order by an attorney authorized to investigate and prosecute the crimes which are the subject of the order. Of course, more than one supervising attorney may be identified.

(iv) the identity of the person, if known, whose communications are to be intercepted;

Commentary to Standard 2-4.2(a)(iv)

This provision is taken from Standard 2-5.3(c) of the Second Edition, and substitutes "are to be intercepted," for "are to be or which were overheard or recorded." This change is stylistic. Note that a person is "known" for purposes of this provision only if there is probable cause to believe the person has, is, or is about to commit the crime which is the subject of the order, and will be intercepted in communications relevant to that crime.94 Note also that for conventional electronic surveillance orders, relevant communications between two persons who are not

---

identified in an electronic surveillance order may be intercepted, since one or both may be an "unknown" agent or co-conspirator in the crime that is the subject of the order.\textsuperscript{95} Indeed, often one of the most important results of electronic surveillance is the identification of previously unknown co-conspirators. For so-called "roving" taps and bugs, however, at least one person must be identified, and only communications to which an identified person is a party may be intercepted. See Standard 2-4.10 and its commentary.

\textbf{(v) the particular offense which is the subject of the electronic surveillance order;}

\textit{Commentary to Standard 2-4.2(a)(v)}

Standard 2-5.3(d) of the Second Edition requires "a specification of the particular offense which is or was under investigation." The change is stylistic.

\textbf{(vi) the objectives of the electronic surveillance;}

\textit{Commentary to Standard 2-4.2(a)(vi)}

Like Title III, the previous editions of the Standards did not include a requirement that the application set forth the objectives of the electronic surveillance, but such a requirement was implicit in Standard 2-5.8(l) of the Second Edition, which required that an electronic surveillance order contain "a statement of the maximum period of overhearing or recording, which shall not be longer than necessary to accomplish the objective of the overhearing or recording warranted by the showing of probable cause . . . ."\textsuperscript{96} A statement of the objectives of the electronic surveillance was also necessary in order to demonstrate in the application, as required by Standard 2-5.3(i) of the Second Edition, that "other investigative procedures . . . have been tried and have failed or reasonably appear to be

\textsuperscript{95} See 1 Carr, \textit{The Law of Electronic Surveillance} (2000), at 5-12.

\textsuperscript{96} Standard 5.8(vi) of the First Edition required only a statement of "the period of authorized or approved overhearing," and made no reference to the "objective of the overhearing or recording." Standard 5.9, however, provided that an electronic surveillance order should require "that overhearing or recording . . . terminate when the objective is achieved . . . ."
unlikely to succeed if tried or to be too dangerous,” since this provision required the applicant to show that these measures had not and reasonably could not achieve the objectives of the investigations.97 Title III includes comparable provisions which also make a statement of the objectives of the electronic surveillance implicitly necessary.98

Explicitly requiring a statement of objectives achieves two important purposes. First, it makes it unnecessary for the objectives to be inferred from the statement of facts contained in the application, as the intercepting officers, the supervising prosecutor, the judge issuing the order, and any suppression or appellate court would otherwise have to do. Second, it effectuates the requirement, newly contained in Standard 2-4.8 of the Third Edition, that the judge issuing the order approve the objectives of the electronic surveillance, “as those objectives are set forth in the application pursuant to Standard 2-4.2(a)(vi).”

(vii) the particular kind of communications sought to be intercepted;

Commentary to Standard 2-4.2(a)(vii)

The change from Standard 2-5.3(e), which requires “a particular description of the type of communications sought to be or which were overheard or recorded,” is stylistic.

(viii) a particular description and the location of the facilities over which or the place where the communications are or will be occurring, or the facts demonstrating that specification of the facility or place is not practical;

97. There is no comparable provision in Standard 5.3 of the First Edition of the Standards, which concerned the form and contents of an application for an electronic surveillance order, but Standard 5.4 of that edition required that the “[t]he statement of facts relied upon by the applicant . . . establish probable cause to believe that . . . (iii) other investigative procedures have or had been tried and have or had failed or reasonably appear or appeared to be unlikely to succeed if tried or to have been or to be too dangerous.”

98. 18 U.S.C. § 2518(5) (providing that “[n]o order . . . may authorize or approve the interception of any wire or oral communication for any period longer than necessary to achieve the objective of the authorization . . . “); 18 U.S.C. § 2518(1)(c)(requiring that application contain “a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they appear to be unlikely to succeed if tried or to be too dangerous”).
Commentary to Standard 2-4.2(a)(viii)

Describing the “facilities over which . . . the communications are or will be occurring” means specifying the service provider and, for a conventional telephone, the telephone line; for a cellular or mobile telephone, the electronic serial number or mobile account number; and for an electronic communication service provider, the customer or subscriber’s account number. Providing the “location” of such facilities is obviously possible only when the facilities are fixed in a permanent location, as when a non-mobile telephone is located on a premises. Describing the place where the communications “are or will be occurring” means specifying the premises or other location where face to face communications are to be intercepted.

In addition to making stylistic changes from Standard 2-5.3(f) of the Second Edition, this provision adds as an alternative to including in the application a description of the facilities or place, providing “the facts demonstrating that specification of the facilities or place is not practical.” This new language is necessary because Standard 2-4.10 permits the issuance of an order not specifying a facility or place when such a demonstration is made. See the commentary to that Standard.

(ix) the period of time for which eavesdropping authority is sought, including a statement that the authorization should not automatically terminate when the described type of communication has been first intercepted, if authority to intercept additional communications is sought;

Commentary to Standard 2-4.2(a)(ix)

This provision is derived from Standard 2-5.3(g) of the Second Edition, which required a statement of “the expected or actual period of time of the overhearing or recording.” The change is stylistic. When the applicant sought authority to intercept additional communications after the first pertinent communication was obtained, Standard 2.5.3(g), like 18 U.S.C. § 2518(d), required “a particular description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter.” The reference to that particular probable cause showing has been moved in the Third Edition to Standard 2-4.3, where it more logically belongs. The requirement that the applicant make that showing is encompassed in subdivision (x), immediately below.
(x) the material facts known to the applicant and necessary for the judge to determine whether the probable cause requirements set forth in Standard 2-4.3 have been satisfied;

Commentary to Standard 2-4.2(a)(x)

This provision is derived from Standard 2-5.3(h) of the Second Edition, which required "a complete statement of the facts relied upon by the applicant warranting the issuance of an order of authorization or approval." The modifications that have been made are meant to clarify the meaning of this provision in several respects. First, when the Second Edition required the inclusion of a "statement of the facts warranting the issuance of the order," it referred to those facts that provided the probable cause showings necessary for the order to be issued. Standard 2-4.2(a)(x) simply makes that reference explicit. Second, by requiring "a complete statement" of those facts, the Second Edition unintentionally suggested that an application that omitted an immaterial fact would not comply with this provision because it was incomplete. More sensibly, the Third Edition requires only a statement of "the material facts known to the applicant and necessary for the judge" to make the requisite probable cause showings. While thus clarifying what facts the applicant must include, this provision, as modified, does not intend to substantively reduce the applicant's obligation to provide the judge with the relevant facts. A Franks challenge may, of course, be made to an application, alleging that false statements of fact were intentionally or recklessly made in the application, or true statements of fact were intentionally or recklessly omitted, which are material to the showings requisite to issuance of the order.99 Third, by referring to the facts "known to the applicant," rather than those the applicant has "relied upon," the present language precludes an applicant from arguing that, although he or she was aware of facts material to probable cause, they were omitted from the application because the applicant was not "rel[ying] upon" them.

(xi) the material facts necessary for the court to determine whether other investigative procedures have been tried and have

failed or reasonably appear to be unlikely to succeed if tried or too dangerous;

**Commentary to Standard 2-4.2(a)(xi)**

This provision is derived from Standard 2-5.3 of the Second Edition, which required a full and complete statement of other investigative procedures that have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous. As with the previous subdivision, and for the same reason, the requirement has been changed from "a full and complete statement" to "the material facts necessary for the court" to make its determination. Thus, a trivial omission in the application concerning an investigative step that was or might have been taken would not violate this provision. See Standard 2-4.2(c), which requires that the statement of fact "relied upon and submitted by the applicant" contain this showing.

(xii) the material facts known to those authorizing and making the application concerning such applications made within the past ten years for the authority to conduct electronic surveillance of the person whose communications are to be intercepted and the facilities over which or the place where the communications to be intercepted are or will be occurring, including, where the application is for the extension of an order, a statement setting forth the results thus far obtained from the electronic surveillance, or a reasonable explanation of the failure to obtain such results; and

**Commentary to Standard 2-4.2(a)(xii)**

This provision is derived from Standard 2-5.3(j) of the Second Edition, which required "a recitation of all facts concerning previous applications . . . ." As with the previous two subdivisions, and for the same reason, the language was changed to require the applicant to include only the "material facts" concerning such applications. Standard 2-5.3(j) of the Second Edition also required, in the case of an "application for the extension of an order, a statement setting forth the results thus far obtained from the overhearing or recording, or a reasonable explanation for the failure to obtain such results." This language has no counterpart in Title III [see 18 U.S.C. 2518(1)(e)], but information concerning the results obtained in executing an electronic
surveillance order would, in any case, be necessary in the application for an extension of that order.

For purposes of this provision, material facts "known" to an applicant include facts the applicant could know with due diligence. At the very least, "due diligence" requires an applicant to maintain retrievable records concerning applications made by the applicant's own office. See Standard 2-3.1(c)(5)(A). When an applicant is generally aware of previous electronic surveillance conducted under the authority of another applicant in another jurisdiction, the applicant should disclose the material information he or she possesses, but, depending on the circumstances, "due diligence" would not necessarily require the applicant to seek out more detailed information concerning that previous electronic surveillance. Obtaining such information would be appropriate if the information contained in the present application were derived from the previous electronic surveillance, or if the applicant for the previous electronic order was a participant in the current investigation. In determining what "due diligence" requires, courts should be guided by the purpose of requiring the applicant to disclose prior applications, that is, preventing the applicant from abusing his or her authority by making repeated and unnecessary applications for electronic surveillance directed at the same subject or subjects. Such abuse cannot be intended when the applicant is unaware of the previous electronic surveillance.

The requirement that information be supplied concerning only those applications made in the past ten years is new. This change conforms the disclosure requirement to the obligation that orders and applications be maintained only for a ten year period (see Standard 2-4.13), and because it is extremely unlikely that a prior application will be relevant in determining whether an order should issue more than ten years later.

(xiii) the need for particular electronic communication service providers and landlords, custodians, or other persons, if known, to furnish information, facilities, or technical assistance, if such is necessary in the execution of the order.

Commentary to Standard 2-4.2(a)(xiii)

This provision is derived from Standard 2-5.3(k) of the Second Edition, which required "a statement of the need for telephone or telegraph companies, landlords, custodians, or other persons" to furnish such assistance. By making reference to "electronic communication service pro-
providers,” a term defined by Standard 2-2.1(g) as “person[s] or entit[ies] which, in the ordinary course of business, routinely [provide] a service allowing [their] users to send or receive private communications,” the provision, as modified, is not limited to telephone and telegraph companies, but extends to those who furnish any type of electronic communication services.

(b) The judge to whom the application is submitted should be permitted to require that additional facts be furnished under oath or affirmation, which should be duly recorded.

Commentary to Standard 2-4.2(b)

This provision is taken from Standard 2-5.3 of the Second Edition, which made reference to the “judicial officer” rather than the “judge,” and which specified that the judicial officer should be permitted to require that the applicant furnish additional facts. Consistent with federal law, the present provision omits the reference, here and elsewhere, to a “judicial officer” to make clear that a federal magistrate judge, or equivalent state or local official, should not be authorized to issue an electronic surveillance order.100 This provision has also been modified to make clear that someone other than the applicant could furnish the additional facts the judge required.

Standard 2-4.3. Probable cause; kinds of showings

The statements of facts relied upon and submitted by the applicant should establish:

(a) probable cause to believe that a person is committing, has committed, or is about to commit a particular designated offense;

Commentary to Standard 2-4.3(a)

The previous editions of the Standards have differentiated between an application for an order authorizing electronic surveillance “for an extended period” and one seeking such authority for “a brief period.”

100. “Senate Report No. 1097 indicates that surveillance orders are not to be issued by United States Magistrates, and district judges cannot delegate authority to issue surveillance orders to magistrate judges.” 1 Carr, The Law of Electronic Surveillance (2000), at 4-110 (footnotes omitted).
2-4.3(a) Electronic Surveillance of Private Communications

For a period of brief surveillance, the probable cause showing was the same as in the present Standard. For an extended period of surveillance, however, Standard 5.4(i)(A) of the First Edition required a showing of probable cause that "the person [who is the subject of the electronic surveillance] is presently or was then engaged over a period of time in the commission of a particular offense with two or more close associates as part of a continuing criminal activity." Standard 2.5.4(a)(ii) of the Second Edition retained this requirement for extended period of surveillance, and increased the requisite number of "close associates" to "three or more." The commentary to the Second Edition noted the increase, but offered no explanation for it. The commentary to Standard 5.4(1) of the First Edition explained that the distinctive showing for extended electronic surveillance was "designed to limit this sort of surveillance primarily to use in the area of organized crime or subversive activity." The commentary to the Standard 2-5.4(a) of the Second Edition offered a slightly different explanation: that "[t]his should limit protracted surveillance primarily to investigations of complex crimes."

A comparable probable cause requirement for "extended surveillance" has never been required under federal law, and it is omitted from the present Standard because the showing of "three or more close associates" engaged in "a continuing criminal activity" is not the only kind of showing that might justify an "extended period" of electronic surveillance. For example, extended surveillance should be permitted if it is necessary to gather evidence against two people, or even one, plotting a single murder. A court issuing an electronic surveillance order may, of course, decide that the probable cause showing made in an application does not justify electronic surveillance for the period requested, and retains the discretion to authorize a shorter period. See Standard 2-4.6(b)(i).

(b) probable cause to believe that evidence concerning that particular offense may be obtained through electronic surveillance of the facilities over which or at the place where the communications to be intercepted are or will be occurring, unless, pursuant to Standard 2-4.10, the facility or place need not be specified;

Commentary to Standard 2-4.3(b)

This provision is drawn from Standard 2-5.4(b) of the Second Edition, which required a showing of probable cause to believe that "facts concerning that particular offense could have been or may be obtained
through an overhearing or recording from the facilities over which or at
the place where such communications are to be overheard or recorded." In
addition to making a number of stylistic changes, the present provi-
sion more accurately refers to the acquisition of "evidence" rather than of "facts." The present provision also adds an exception for an applica-
tion for an order issued pursuant to Standard 2-4.10 which does not
specify a facility or place. In such a case, the facts set forth in the appli-
cation must nonetheless furnish probable cause to believe that evidence
concerning the offense which is the subject of the order may be obtained
by the "roving" electronic surveillance sought by the applicant. See the
commentary to Standard 2-4.10.

(c) that for purposes of achieving the objectives of the electronic
surveillance as described in the application, other investigative pro-
cedures have been tried and have failed or reasonably appear to be
unlikely to succeed if tried or to be too dangerous; and

Commentary to Standard 2-4.3(c)

The First and Second Edition of the Standards imposed the same
requirement of necessity, using almost identical language. Specifically,
Standard 2-5.4 of the Second Edition provided that the "statement of
facts relied upon and submitted by the applicant should establish prob-
able cause for the belief that: . . . (c) other investigative procedures have
or had been tried and have or had failed or reasonably appear or
appeared to be unlikely to succeed if tried or to have been or to be too
dangerous." The present version of the Standards (like Title III) omits
the reference to "probable cause," since, even without it, other inves-
tigative procedures must either "have been tried and have failed,"
or they must "reasonably appear to be unlikely to succeed if tried or to
be too dangerous." Requiring that it be "probable" that something "rea-
sonably appear to be unlikely" is, at best, redundant, and, at worst,
creates a complex and inexplicable two-prong standard. The present
version also makes explicit what was previously implicit: that neces-
sity of the electronic surveillance must be determined "for purposes of
achieving the objectives of the investigation." As previously indicated
in the commentary to Standard 2-3.1(c)(i)(C), the objectives should be
reasonably achievable given the probable cause showings made in the
application.
In similar language, Title III also provides that in order to obtain a warrant for the interception of wire, oral, or electronic communications, the applicant must demonstrate that "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous. " 18 U.S.C. 2518(c). This requirement of "necessity" is sometimes referred to as the "exhaustion" requirement, a term which misleadingly suggests that all alternatives to electronic surveillance must actually be attempted before an eavesdropping warrant may issue. For purposes of this provision, an investigative procedure is "too dangerous" if it would create a danger of physical harm, and it is "reasonably unlikely to succeed if tried" if attempting it could jeopardize the objectives of the investigation. In considering whether necessity has been demonstrated, courts attempt to make a commonsense and practical evaluation of the adequacy of the showing.

101. Concerning the necessity requirement see, Carr, The Law of Electronic Surveillance (2000), at 4-64, et seq. "Normal investigative procedure would include, for example, standard visual or aural surveillance techniques by law enforcement officers, general questioning or interrogation under an immunity grant, use of regular search warrants, and the infiltration of conspiratorial groups by undercover agents or informants." Senate Report No. 1097, 90th Cong., 2d Sess., 1968 U.S. Code Cong. & Admin. News 2122, 2190 (1968). The 10th Circuit has held that pen registers and trap and trace devices are also among the normal investigative techniques which must be considered before eavesdropping is employed "because they possess a logical relationship and close affinity to wiretaps and yet are less intrusive," United States v. Castillo-Garcia, 117 F.3d 1179, 1187-88 (10th Cir. 1997), and that in particular cases, other normal investigation techniques appropriate to that case need be considered as well, including for example, obtaining telephone toll records and "reviewing available public, private or governmental records pertaining to the suspects." 117 F.3d at 1188.

102. See, e.g., United States v. Edwards, 69 F.3d 419, 429 (10th Cir. 1981) ("In examining necessity challenges to wiretap orders, we have repeatedly held that law enforcement officials are not required to exhaust all other conceivable investigative procedures before resorting to wiretapping"). As one court has explicitly observed, "the government may obtain a wiretapping warrant without trying any other method of investigation, if it demonstrates that normal investigatory techniques reasonably appear to be unlikely to succeed if tried, or to be too dangerous to try." United States v. Castillo-Garcia, 117 F.3d 1179, 1187 (10th Cir. 1997). See also United States v. Vento, 533 N.2d 838, 849 (3d Cir. 1976) ("There is no requirement that every investigative methodology be exhausted prior to application for [an eavesdropping warrant]. Investigators are not obliged to try all theoretically possible approaches. It is sufficient that the government show that other techniques are impractical under the circumstances and that it would be unreasonable to require pursuit of those avenues of investigation.") (footnotes omitted). See also US v. Spagnuolo, 549 F.2d 708 (9th Cir. 1977).
while still demanding that it be particularized to the facts and circumstances of the investigation. The Standards' approach to the necessity requirement is the same.

Application of the necessity requirement can become problematic when an applicant seeks authority for electronic surveillance of communications occurring in more than one place and/or over more than one facility for the transmission of private communications. The problems multiply when the surveillance sought includes the interception of more than one kind of electronic communication (for example, both telephone conversations and e-mail). While the language of the necessity requirement is not explicit in this regard, an applicant should, of course, exercise discretion in determining whether the objectives of the electronic surveillance can still be achieved if the electronic surveillance sought does not include every place or facility for which a probable showing could be made. The questions that should be asked are whether it is probable that different evidence could be obtained by the interception of private communications at an additional place or facility, and whether that additional evidence is likely to be necessary in order to achieve the objectives of the investigation. Standard 2-7.1(ii) offers some guidance to the applicant, by stating that a law enforcement agency should adopt administrative regulations that "specify the circumstances under which [electronic surveillance] may be used, giving preference to those which invade privacy least." The Standards also give a role to the judge, by providing that "when the authorization is sought to intercept communications occurring in more than one place and/or over more than one facility," the judge should be authorized to

103. Compare United States v. Oriakhi, 57 F.3d 1290, 1298 (4th Dep't. 1995) (noting that "as we have repeatedly held 'the burden that these provisions impose upon the government to show the inadequacy of normal investigative techniques is not great, and the adequacy of such a showing is 'to be tested in a practical and commonsense fashion,' . . . that does not 'hamper unduly the investigative powers of law enforcement agents,'""); quoting and omitting citations from People v. Smith, 31 F.3d 1294, 1297 (4th Cir. 1994), with United States v. Robinson, 698 F.2d 488, 453 (D.C. Cir. 1983) ("The affidavit must show with specificity why in this particular investigation ordinary means of investigation will fail.") (emphasis in original), quoted with approval, United States v. Carrazana, 921 F.2d 1557, 1565 (11th Cir. 1991); People v. Ippolito, 744 F.2d 1482, 1486 (9th Cir. 1985). See also United States v. Lilla, 699 F.2d 99, 105 (2d Cir. 1983) (holding that eavesdropping warrants should not have been issued because wiretap was not necessary, but merely a useful additional tool).
grant either all of the authority requested, or only part of it. Standard 2-4.6(b)(vi).\textsuperscript{104}

Because Title III offers greater protection to communications that include the human voice than to those that do not, it might be argued that Congress viewed the interception of wire and oral communications as more invasive of privacy than the interception of electronic ones, and that if the objectives of an investigation could be achieved by either the interception of electronic communication or by the interception of aural ones, only the latter should be authorized. Since the Standards offer the same level of protection to all forms of private communication, however, they express no preference that the interception of any particular form be attempted or considered before application for authority to intercept another is made. Whether, for example, the interception of both oral and electronic communications is necessary, whether the interception of one is more intrusive than the interception of the other, and whether the interception of one but not the other is practical (since both may be transmitted over the same facilities), will necessarily turn on the facts of each case.

Moreover, since Title III applies only to the interception of communications, and not to video surveillance which captures only images and not the human voice, it could also be argued that Congress meant for applicants for audio surveillance to be required to first use video surveillance, or explain why it would be too dangerous to try or unlikely to succeed. However, Standard 2-9.3 of the Standards on Technologically-Assisted Physical Surveillance provides that video surveillance of a private activity or condition should be permissible “when it complies with provisions applicable to electronic surveillance of communications.”\textsuperscript{105}

Thus, under that Standard, an application for video surveillance must demonstrate necessity for the surveillance in the same manner that necessity must be established for electronic surveillance of private communications. When probable cause exists for both audio and video surveillance, the question thus arises whether one is more intrusive than the other, and whether one should be attempted or considered before an

\textsuperscript{104} See United States v. Castillo-Garcia, 117 F.3d 1179, 1196 (10th Cir. 1997) (“even within an ongoing investigation of a suspected drug conspiracy, the government may not simply ‘move swiftly from wiretap to wiretap.’ . . . Rather, under Title III, it must always ‘pause[e] to consider whether normal investigative procedures could be used effectively, particularly in light of an evidence obtained as a result of each succeeding wiretap’”) (citations to suppression court opinion omitted).

\textsuperscript{105} For the definition of a private activity or condition, see Standard 2-9.2(f) of the Standards on Technologically-Assisted Physical Surveillance.
application for the other is made. In some cases, the question of whether audio or video surveillance is more intrusive will not arise because the application is for both and the applicant can establish that both are necessary. When both are not necessary, however, a comparison of their relative intrusiveness should be made and resolved on a case by case basis. One form of surveillance may clearly be more intrusive than the other, when, for example, the video surveillance contemplated is of activity occurring in a bedroom, and the audio surveillance of a business telephone. As with applications for electronic surveillance of multiple places and/or facilities, discretion by the applicant is called for, as is review by the judge to whom the application is made.

(d) if the nature of the investigation is such that the authorization should not automatically terminate when the described type of communication has been first obtained, probable cause to believe that additional communications of the same type will occur thereafter.

Commentary to Standard 2-4.3(d)

This provision is taken from Standard 2-5.3(g) of the Second Edition, and contains only stylistic changes from the language there. It was moved here because it concerns the general subject matter of this Standard, that is, the probable cause showings that must be made in an application for an electronic surveillance order.

Standard 2-4.4. Designated offenses; criteria

An application for an order authorizing electronic surveillance should be permitted only for the investigation of offenses which are

106. As the commentary to Standard 2-9.3 of the Standards on Technologically-Assisted Physical Surveillance indicates, it would be absurd to conclude from the fact that both require a showing of necessity that audio and video surveillance are prohibited in any case where either is likely to succeed in achieving the objectives of the surveillance. In such circumstances, either should be permissible if the necessity requirement is otherwise met.

107. One court has concluded that video surveillance is more intrusive than the interception of oral communications, and has held—despite the absence of any comparable statutory requirement of necessity applicable to it—that “[t]he showing of necessity needed to justify the use of video surveillance is higher than the showing needed to justify other search and seizure methods, including bugging,” United States v. Mesa-Rincon, 911 F.2d 1433, 1442 (10th Cir. 1990).
punishable by more than one year imprisonment and have been designated by the legislature as serious enough to justify the intrusiveness of the surveillance.

Commentary to Standard 2-4.4

From its inception, Title III has limited the offenses for which electronic surveillance of wire and oral communications may be authorized. Within the constraints of these limitations, however, electronic surveillance for a broad range of crimes is permitted.\textsuperscript{108} A federal applicant may apply for an order authorizing such electronic surveillance in connection with a long list of federal offenses enumerated in 18 U.S.C. 2516(1). While the list has since been lengthened, the commentary to Standard 2-5.5 of the Second Edition of the Standards described these offenses as “roughly divided into three categories: national security offenses, intrinsically dangerous crimes, and activities characteristic of organized crime.” Federal orders authorizing the interception of electronic (non-aural) communications, however, may be issued in connection with the investigation of “any Federal felony.” 18 U.S.C. § 2516(3).

Unable, as it could for federal offenses, to enumerate specifically the offenses which could be the subject of a state or local application for an electronic surveillance order, Congress generically limited state orders—for the interception of electronic communications, as well as for wire and oral ones—to “murder, kidnapping, gambling, robbery, bribery, extortion, or dealing in narcotic drugs, marijuana or other dangerous drugs, or other crimes dangerous to life, limb, or property, and punishable by imprisonment for more than one year.” 18 U.S.C. 2516(2). The commentary to Standard 5.5 of the First Edition of the Standards described offenses like murder and kidnapping as offenses that were “serious in themselves,” and extortion, bribery, gambling and narcotics offense as those that are “characteristic of group activity.” A number of courts have held that the requirement that an offense be “punishable by imprisonment for more than one year” is applicable to those “crimes dangerous

\textsuperscript{108} “Although it is generally acknowledged that court-ordered eavesdropping is necessary and useful only for the investigation of particular types of serious offenses, [Title III] authorizes court-ordered electronic surveillance across an extremely broad range of federal crimes and an even broader range of state offenses, thereby creating a substantial risk of excessive eavesdropping.” 1 Carr, The Law of Electronic Surveillance (2000), at 4-4.
Electronic Surveillance of Private Communications

2-4.4

to life, limb or property," and not to "murder, kidnapping, gambling, robbery, bribery extortion, or dealing in narcotic drugs, marijuana or other dangerous drugs," thus permitting misdemeanor gambling, bribery and narcotic offenses to be the subject of state electronic surveillance orders.109 The commentary to the Second Edition of the Standards notes that "States that authorize court-ordered electronic surveillance have varied greatly in their enumerations of offenses."110

The First and Second Edition of the Standards followed Congress in limiting electronic surveillance of aural communications to designated offenses, and by providing, more simply than does Title III, that the offenses designated "should be serious in themselves or characteristic of group activity." See Standard 2-5.5 of the Second Edition. The Third Edition, however, has taken a somewhat different approach by permitting federal and state applications "only for the investigation of offenses which are punishable by more than one year imprisonment and have been designated by the legislature as serious enough to justify the intrusiveness of the surveillance." The Standard takes its present form for a number of reasons. First, the requirement that designated offenses be "serious in themselves" is too vague to provide guidance beyond that supplied by the limitation that they be "punishable by more than one year imprisonment." Second, it is the position of the Standards that the intrusiveness of electronic surveillance is not justified for the investigation of misdemeanors, even misdemeanors that are of a type "characteristic of group activity." Third, even in determining what kind of felonies warrant the use of electronic surveillance, demanding that they be "characteristic of group activity" does not provide meaningful guidance, and is, of course, irrelevant in determining whether electronic surveillance is justified in the investigation of individual acts of economic injury or physical violence. Thus, Standard 2-4.4 leaves to individual legislative determination what felonies are "serious enough to justify

109. Other courts have held to the contrary. For a collection of decisions holding each way, see 1 Carr, The Law of Electronic Surveillance (2000), at 4-10-4-11.

110. Commentary to Standard 2-5.5 of the Second Edition (footnote omitted). "At one extreme, Arizona, Connecticut, Georgia, and Utah place practically no restrictions on the offenses that may be investigated by court-ordered surveillance, as their statutes either allow surveillance as to any felony, or as to any felony involving bodily harm. At the other extreme, court-ordered surveillance can be conducted in Alaska only for murder in the first or second degree, kidnapping and certain felony-level drug offenses." 1 Carr, The Law of Electronic Surveillance, at 4-7 (footnotes omitted).
the intrusiveness of [electronic] surveillance."111 Fourth, the Standard rejects for this purpose, as for all others, treating aural communications differently from non-aural ones, and thus does not follow federal law in establishing one set of criteria for offenses that may be the subject of electronic surveillance of wire and oral communications, and another for those that may be the subject of electronic surveillance of electronic communications.

Standard 2-4.5. Other offenses

(a) When, during lawfully conducted electronic surveillance, communications are intercepted which relate to offenses other than those specified in the initial surveillance order, whether or not those offenses are among the designated offenses for which such surveillance may be authorized, and the contents were obtained lawfully:

(i) the contents of those communications and evidence derived therefrom may be disclosed or used by law enforcement officers and officials to the extent such use or disclosure is appropriate to the proper performance of official duties; and

(ii) the contents of those communications and evidence derived therefrom may be introduced into evidence.

Commentary to Standard 2-4.5(a)

From its inception, 18 U.S.C. 2517(5) has provided that when communications are intercepted "relating to offenses other than those specified in the order of authorization or approval," their contents, and evidence derived from their contents, may be used "when authorized or approved by a judge of competent jurisdiction where such judge finds on subsequent application that the contents were otherwise intercepted in accordance with the provisions of this chapter." Similarly, Standard 2-5.6(a) of the Second Edition requires that "when conversations... which relate to offenses other than those specified in the initial surveillance order" are intercepted, they may be disclosed, used, and introduced into evidence only if "a judge authorized to issue surveillance

111. Beyond that, Standard 2-3.1(c)(i)(B) directs an applicant, in determining whether to apply for an order authorizing electronic surveillance in connection with a felony a legislature has so designated, to consider whether that felony, as it has been, is being or is about to committed in that particular case, warrants the intrusiveness of the electronic surveillance being contemplated.
orders finds upon subsequent application that the contents were obtained lawfully." The Third Edition of the Standards abandons the requirement of obtaining such a retrospective order.

As the commentary to Standard 5.6 of the First Edition of the Standards makes clear, the requirement for a "retrospective amendment" of an electronic surveillance order arose from concern about the continuing vitality of *Marron v. United States*, in which the Supreme Court held that the "particularity" requirement of the Fourth Amendment made it unlawful to make a "seizure of one thing under a warrant describing another." 112 In *Coolidge v. New Hampshire*, however, the Court held that officers executing a conventional search warrant could seize property not described in the warrant if they observed the property in plain view and came across it inadvertently. 113 Because *Coolidge* does not require either a prospective or retrospective court order for a "plain view" seizure, the retrospective order required by Title III and the earlier editions of the Standard is not constitutionally necessary. The question remains whether it would be useful to require nonetheless that an applicant obtain a retrospective order approving the seizure of a communication that relates to an offense other than one specified in the order that authorized the electronic surveillance.

Under Title III and comparable state provisions, a variety of problems have arisen in determining when the retrospective amendment of an electronic surveillance order is required. For example, is a retrospective amendment necessary when a communication is seized which is not only evidence of an offense which is the subject of an electronic surveillance order, but of other crimes as well? Is a retrospective amendment necessary if evidence is sought and obtained as evidence of a state crime, but is then used in the prosecution of a related offense? When a communication is intercepted relating to an offense which is not the authorized subject of an electronic surveillance order, must a retrospective amendment be obtained if the crime to which the communication does relate is not a "designated offense" for which prospective authority for its seizure could have been issued? May a retrospective amendment approving the interception of a communication relating to an

---


113. 403 U.S. 443 (1971). Concerning the abandonment of the inadvertence requirement, see the commentary to Standard 2-4.5(c).
Electronic Surveillance of Private Communications

non-designated offense be obtained? Federal and state courts have often given inconsistent answers to these and related questions. Federal law, like the previous editions of the Standards, requires that an application must be made "as soon as practicable," and federal courts—but not always their state counterparts—have read this provision generously, leaving the law concerning when application for a retrospective amendments must be made exceeding unclear.

Since any communication that could be the subject of a retrospective amendment has, by definition, already been acquired, a contemporaneous determination by the judge of the lawfulness of its acquisition cannot "undo" the interception of that communication. It can, however, prospectively effect the manner in which an electronic surveillance order is executed. Thus, embodied in the requirement of an application for a retrospective amendment, and in the requirement that the application be made as soon as practicable, is "the principle of ongoing judicial supervision" of the execution of an electronic surveillance order. This principle is equally well served, and the complications attendant to the obligation of obtaining a retrospective amendment avoided, if such an amendment is not required, but the judge must nevertheless be given notice of the interception of communications unrelated to the crime which is the subject of the order. Armed with such notice, the judge will be alert to issues concerning the interception of unrelated communica-


115. Compare United States v. Arnold, 773 F.2d 823 (7th Cir. 1985) (application made 31 months after termination of interception not untimely), with People v. Winograd, 68 N.Y.2d 383 (1986) (application for retrospective amendment untimely when made eighteen days after probable cause existed that intercepted conversations related to another crime). By statute, a retrospective amendment to an electronic surveillance order issued by a Wisconsin state court judge must be filed within forty-eight hours, Wis. Stat. Ann. § 968.29(5) (West Supp.). See, generally, 1 Carr, The Law of Electronic Surveillance (2000), at 5-72-5-79. Particular difficulty in determining the timeliness of an application arises when the information establishing probable cause that a communication is evidence of another crime results from information obtained after—perhaps often long after—the communication is intercepted. Those conducting the investigation may not even recall the communication at the time the new information is obtained, and thus its relevance to the crime may remain undiscovered until the communication is rediscovered and its significance reconsidered. Gauging the timeliness of an application to use the communication based upon when the new information was obtained—rather than upon when the connection was made between it and the previously intercepted communication—seems unduly harsh.

tions, and can issue instructions concerning their interception in the future. The Third Edition of the Standards adopts this approach by abolishing the requirement for retrospective amendments, but requiring that a judge who issues an electronic surveillance order periodically receive progress reports concerning the execution of that order, and that the progress reports include notice of the interception of any such communications and of their contents. Standard 2-4.8(m).

By abolishing the requirement of retrospective amendments, the Standards do not, of course, suggest that intercepted communications that are unrelated to a crime which is the authorized subject of the electronic surveillance should always be permitted in the prosecution of another unrelated crime. As the previous editions of the Standards required for a retrospective amendment, Standards 2-4.5 still requires that the communication must have been intercepted “during lawfully conducted surveillance,” and that the contents of the communication itself must have been “obtained lawfully.” Should the use of such a communication be sought at trial, or of evidence derived from it, the defendant against whom it is offered may challenge the lawfulness of its interception. Failure to disclose the interception of a communication in a progress report could be a factor in determining whether suppression is appropriate. Standard 2-4.5(a) makes clear that a communication relating to an offense not the subject of an electronic surveillance order may lawfully be intercepted “whether or not [the offense is] among the designated offenses for which such surveillance may be authorized.”

(b) When evidence of another designated offense has been intercepted, and the officers desire to obtain specific authority to intercept future communications relating to that offense, an application in conformity with Standards 2-4.1 through 2-4.4 should be made and approved.

Commentary to Standard 2-4.5(b)

The subject matter of this provision is the issuance of a prospective, rather than retrospective, amendment of an electronic surveillance order, that is, the issuance of an order that would authorize law enforcement officers executing an electronic surveillance order to intercept communications related to an offense that by law is designated as one for which such an order could issue, but was not the subject of the order which the officers were executing. If the offense to which the communications
relates is not a designated offense for which an electronic surveillance order could have issued, a prospective amendment authorizing the interception of communications relating to that offense may not be issued. This provision is derived from Standard 2-5.6(b) of the Second Edition of the Standards and includes changes that are meant to clarify its meaning but not to alter its substance.

(c) When evidence of another designated offense has been intercepted, and an application to intercept future communications constituting evidence of that offense has not been made pursuant to Standard 2-4.5(b), future communications relating to that other offense may nonetheless be intercepted in conformity with Standard 2-4.5(a).

Commentary to Standard 2-4.5(c)

During the execution of an electronic surveillance order, even though the officers are aware that communications might be intercepted in the future relating to an offense not the subject of that order, the applicant for the order might not be able to obtain a prospective amendment pursuant to Standard 2-4.5(c) authorizing the interception of future communications relating to that other offense. Such an order might not be obtainable because the applicant is unable to demonstrate probable cause that future communications relating to the new crime will occur, because the offense is not a "designated" one for which electronic surveillance may be authorized, or because the applicant is unable to demonstrate that the new crime cannot be investigated by other means. Even if all the requirements for a prospective amendment are met, the new offense may not be one for which the applicant deems electronic surveillance worthwhile.\(^\text{117}\) In each case, the question then arises whether, if such a communication occurs, it may be intercepted by the officers executing the order. The answer provided by Standard 2-4.5(c) is that it may be intercepted, so long as it is in plain view.

Although the officers executing an electronic surveillance order may not search for communications that are evidence of an offense not designated in the order, they may nonetheless intercept such communications if they come across them while appropriately searching for

\(^{117}\) An example of the last possibility might be if the offense named in the electronic surveillance order is murder, and a person is using the same facility over which the murder communications are occurring to place bets which are unrelated to the murder.
communications related to a designated offense. Given that the Supreme Court has held that inadvertence is no longer required for a plain view seizure, communications relating to a crime which is not the subject of an electronic surveillance order may be seized even if the prosecutor could have obtained a prospective amendment authorizing the seizure of those communications but chose not to do so. 118 Neither of the previous editions of the Standards nor Title III has explicitly made "inadvertence" a requirement for a retrospective amendment authorizing the use of a communication relating to a crime which was not the subject of an eavesdropping warrant. 119 Section 2-5.6(a) of the Second Edition of the Standards requires only that such a communication have been "obtained lawfully," and 18 U.S.C. 2518(5) requires only a showing that the communication was "otherwise intercepted in accordance with the provisions of this chapter."

Standard 2-4.6. Judicial discretion and determination

In the exercise of sound discretion:

(a) the judge to whom an application for authorization is submitted should be permitted to deny the application, and

(b) upon determining that the application satisfies the showings required by Standard 2-4.3, the judge should be authorized to grant the order either as requested, or with appropriate modifications, including but not limited to:

(i) reducing the length of the maximum period of authorized electronic surveillance;

(ii) modifying the authorized objectives of the electronic surveillance;

118. In Horton v. California, 496 U.S. 128 (1990), the Supreme Court abandoned the requirement announced in Coolidge v. New Hampshire that for a plain view seizure to be constitutional, the discovery of the evidence must be inadvertent, i.e, the police must not have had probable cause to believe that they would find the property seized when they searched for the property particularized in the warrant. In United States v. Bankston, 182 F.3d 296, 307-08 (5th Cir. 1999), the court held that inadvertence was also not required in order to intercept a communication in plain view during court-ordered electronic surveillance.

119. State courts, may, of course, decline to follow Horton as a matter of state constitutional law, see 1 Carr, The Law of Electronic Surveillance (2000), at 5-64.7, and a state may have or enact a statutory provision that make inadvertence a requirement for a plain view seizure of a private communication.
(iii) requiring progress reports, or modifying the frequency with which progress reports, if any, must be submitted;
(iv) specifying or modifying the manner in which records of intercepted communications are to be made;
(v) specifying or modifying the manner in which the minimization of communications not subject to interception is to be achieved, either contemporaneously with or after their interception; or
(vi) when the authorization sought is to intercept communications occurring in more than one place and/or over more than one facility, granting only part of the authority requested.

Commentary to Standard 2-4.6

Federal law provides that a judge “may” issue an electronic surveillance order if the judge determines that the application for the order is legally sufficient. 18 U.S.C. § 2518(3). More explicitly, Standard 2-5.7 of the Second Edition of the Standards provided, in language only stylistically different from that in the First Edition, that the judge to whom an application for an electronic surveillance order is made should “be permitted in the exercise of sound discretion to deny the application, and, if the application established the requisite probable cause, “should be authorized to grant the order as requested or with appropriate modifications.”

The commentary to Standard 2-5.7 of the Second Edition assumed that it was appropriate for a judge “to participate in the formulation of policies relating to the use of electronic surveillance,” and contemplated “situations where, despite a technically adequate showing of probable cause, surveillance should not be authorized when the interests of privacy and law enforcement are balanced.” The present Edition of the Standards cautions the judge to leave to the applicant the task of balancing the importance of the electronic surveillance with its intrusiveness,120 but nonetheless continues to extend a general invitation to the judge to exercise discretion to deny or modify an order, and goes even further, by specifying, without limiting, the kinds of modifications the court might consider making. A number of the suggestions for modifications implement the general principle that the judge who issues an electronic surveillance order “can and should ensure that it is executed appropriately.” Thus the judge could modify the order by increasing the

120. See, e.g., subdivisions (B) and (C) of Standard 2-3.1(c)(i), and the commentary to each subdivision.
frequency of progress reports, or by specifying or modifying the manner in which minimization is to be conducted.

To a significant degree, the discretion afforded by this Standard makes unnecessary other provisions that would have been less flexible and more difficult to apply. For example, the discretion in Standard 2-4.6(vi) to grant authority to intercept communications in fewer than all of the places and/or over fewer than all of the facilities requested by the applicant makes it unnecessary to require a showing of necessity particularized for each place and facility. Similarly, providing that the court may reduce the authorized maximum period of interception makes it unnecessary to retain a provision in the earlier editions of the Standards that required a particularized probable cause showing for long term surveillance. See the commentary to Standard 2-4.3(a).

Standard 2-4.7. Order; jurisdiction

(a) A federal judge should be permitted to issue an electronic surveillance order authorizing the interception of private communications, regardless of where those communications are occurring, if the communications are to be intercepted in the United States, and the offense which is the authorized subject of the electronic surveillance has been, is being, or is about to be committed within the territorial jurisdiction of the court; and

(b) A state judge should be permitted to issue an order authorizing the interception of private communications, regardless of where those communications are occurring, if:

(i) the offense which is the authorized subject of the electronic surveillance has been, is being, or is about to be committed within the territorial jurisdiction of the court in which the judge is sitting, and the communications are to be intercepted within the state; or

(ii) the offense which is the authorized subject of the electronic surveillance has been, is being, or is about to be committed in another state; the communications are to be intercepted within the territorial jurisdiction of the court in which the judge is sitting; and the law of the state in which the judge sits permits the judge to issue such an order;

provided, however, that:

(iii) a state court judge should be permitted to issue an order authorizing the interception of communications occurring between
or among parties known to be outside the state only pursuant to
an interstate compact permitting such interceptions; and

(iv) an electronic communication service provider should be
required to comply with an order issued pursuant to Standard
2-4.8(i) that it furnish information, facilities, or technical assistance
for the execution of an electronic surveillance order to be executed
in a state if:

(A) the provider is lawfully served with the order in that state, or
(B) the provider is lawfully served with the order in another
state and is required to comply with it pursuant to an interstate
compact.

Commentary to Standard 2-4.7

Although the previous editions of the Standards contained no provi-
sion concerning the geographical jurisdiction of an electronic surveillance
order, Title III provides that a judge may enter an order authorizing the
interception of wire, oral or electronic communications “within the terri-
torial jurisdiction of the court in which the judge is sitting.”121 When Title
III was drafted, it made sense to base jurisdiction for the issuance of an
electronic surveillance order on the place where the officers executing an
order would actually intercept the communications. Under the technol-
ogy then prevailing, that place, for a bug, was usually near where the oral
communications were occurring and, for a wiretap, near where the
tapped telephone was located. Now, however, the place where commu-
nications occurring by means of portable devices like pagers, telephones
and computers is constantly changing. More importantly, the nexus
between the place where telephonic and electronic communications are
occurring and where they can be intercepted has seriously eroded. Com-
munications to some pagers and to and from some mobile and cellular
telephones are transmitted throughout a broad geographical area, in
some cases throughout the country, and even the world. Communications
occurring over such devices can be intercepted at any location
within the area in which they are transmitted. Similarly, electronic com-
munications transmitted to and from computers can also be intercepted

121. 18 U.S.C. § 2518(3). “[I]n the case of a mobile interception device authorized by
a Federal court within such jurisdiction,” the judge may authorize the interception of such
communications “outside that jurisdiction but within the United States.” Id. A “mobile
interception device” is a tap on a mobile telephone or a bug in a vehicle. 1 Carr, The Law
of Electronic Surveillance (2000), at 4-126.
Electronic Surveillance of Private Communications

anywhere another computer can be operated. Indeed, present technology permits communications which occur even between two conventional telephones in two fixed locations to be routed to a third location and intercepted there.

Confronted with such technology, courts have held that "a judge can issue a surveillance order authorizing attachment of the surveillance device within his or her territorial jurisdiction, but overhearing in another territorial jurisdiction."\textsuperscript{122} Indeed, regardless of where the parties to the communications are located, "interception" has been deemed to occur where the conversations are 'captured or redirected in any way.'\textsuperscript{123} Given these developments, "any federal district court, circuit court of appeals or appropriate state court may authorize a wiretap any place in the country,"\textsuperscript{124} and the place of interception, standing alone, has become an ineffective basis for setting meaningful geographic limitations on a court's authority to issue an electronic surveillance order. One concern that thus arises is that "law enforcement officials are now able to shop, free from territorial constraints, for a judge who would be likely to authorize a wiretap."\textsuperscript{125} Another concern is that the proliferation of the number of prosecutors who may seek an electronic surveillance order in a particular case may lead to unseemly and counterproductive competition between them.

Standard 2-4.7 offers a different and more carefully nuanced approach to this problem, which is destined only to worsen under present law. Specifically, Standard 2-4.7 makes jurisdiction turn, not on the place of execution, but on the territorial jurisdiction of the issuing judge over the offense which is the authorized subject of the investigation. Pursuant to subdivision (a), a federal judge can issue an order authorizing the

\textsuperscript{122} 1 Carr, The Law of Electronic Surveillance (2000), at 4-125, citing United States v. Ramirez, 112 F.3d 849 (852 (7th Cir. 1997), and United States v. Nelson, 837 F.2d 1519, 1526 (11th Cir. 1988).

\textsuperscript{123} 1 Carr, The Law of Electronic Surveillance (2000), at 4-125, quoting United States v. Rodriguez, 968 F.2d 130, 136 (2d Cir. 1992), in which the court held that "a communication is intercepted not only where the tapped telephone is located, but also where the contents of the redirected communication are first to be heard." See also United States v. Butford, 755 F.Supp. 607 (1991) (district judge in Southern District of New York had jurisdiction to authorize wiretap of telephone located in Maryland whose calls were routed by a "slave" device to a wireroom in New York).

\textsuperscript{124} United States v. Rodriguez 968 F.2d 130, 143 (Meskill, Circuit Judge, concurring).

\textsuperscript{125} United States v. Rodriguez, supra. See also Castillo v. State, 810 W.W.2d 180, 184 (Tex. Crim App. 1990) (en banc) (rejecting such an interpretation of a similar state statute in order to prevent judge shopping).
interception of communications “regardless of where those communications are occurring” so long as two requirements are met: first, the “communications are to be intercepted within the United States”; and second, the offense is being committed “within the territorial jurisdiction of the court.” Thus, pursuant to an order issued by a judge of the Federal District of New York, federal agents can intercept communications in California, even if the communications are occurring in Tokyo (“regardless of where the communications to be intercepted are occurring”).126

Subdivision (b) deals with state applications. Subdivision (i) of that provision permits a judge with jurisdiction over the offense which is the subject of investigation to issue an order authorizing the interception of communications “regardless of where those communications are occurring,” so long as the “communications are to be intercepted within the state.” Thus, if the communications are occurring in Los Angeles, or even in Tokyo, a Florida state judge with jurisdiction over the offense can authorize their interception (if technology permits) “anywhere in the state” of Florida. If interception can only occur outside the state, subdivision (ii) permits a judge of the state in which the communications are occurring to authorize their interception “regardless of where those communications are occurring” so long as two requirements are met: first, the place of interception must be “within the territorial jurisdiction of the court in which the judge is sitting”; and second, “the law of the state in which the judge sits permits the judge to issue an order.” Thus, if these two conditions are met, the state of Kansas can authorize its law enforcement officers to intercept communications relating to a North Dakota crime.

The provisos in subdivisions (iii) and (iv) of Standard 2-4.8(b) deal with two special cases. Subdivision (iii) deals with a situation in which, for example, a New York prosecutor knows that communications relating to a New York crime are occurring between two parties in New Jersey, and technology permits them to be intercepted in New York. The proviso says such out of state communications could “knowingly” be intercepted [pursuant to subdivision (i)] only if permitted by a compact. If someone was traveling in and out of state with a cellular telephone,

126. Although this Standard (and Title III) may permit the interception of these Tokyo communications, the applicant and/or the prosecuting attorney supervising the execution of the order should consider whether their interception violates Japanese law, and if so, whether the communications should be intercepted.
and the intercepting officers did now know whether or when communications were occurring over the phone in or out of state, the proviso would not apply, because the interceptions would not "knowingly" be of out of state communications.

The second proviso, contained in subdivision (iv) of Standard 2-4.8(b), is designed for the situation in which an order could be issued by a state judge pursuant to either subdivision (i) or (ii), but the provider whose cooperation was necessary to execute the order could not lawfully be served with it within the state, and thus its cooperation could not otherwise be mandated by that judge's order. Subdivision (iv) permits service on the provider either in a state, if service in the state is lawful, or out of the state, if such service is permitted by a compact.

Of course, not all states would enact the enabling legislation contemplated by subdivision (ii), or join in either of the compacts contemplated by subdivisions (iii) and (iv), but interstate comity makes these limitations appropriate. In the absence of the necessary legislation or compact, however, another option almost always exists, that is, to enter into a joint investigation with the local United States Attorney and seek a federal electronic surveillance order.

**Standard 2-4.8. Order; form; contents**

The order should be issued in writing signed by the judge and contain the following information:

(a) the identity of the prosecuting official authorizing the application pursuant to Standard 2-4.1(b);

*Commentary to Standard 2-4.8(a)*

This provision is taken from Standard 2-5.8(a) of the Second Edition, which required the application to identify "the prosecuting officer authorizing the application." The term "officer" was changed to "official" because the latter term was deemed more appropriate for principal prosecuting attorneys and their high ranking subordinates. The reference to Standard 2-4.1(b) was added because that provision governs which officials should be permitted to make applications for electronic surveillance orders.

(b) the identity of the prosecuting attorney who will supervise the execution of the order;
Commentary to Standard 2-4.8(b)

This provision is new in the Third Edition of the Standards, and was added to implement Standard 2-3.1(c)(ii)(A), which provides that "the execution of [an electronic surveillance] order should be supervised by an attorney authorized to investigate and prosecute the crimes which are the subject of the order," by requiring that the order identify that attorney. See also Standard 2-4.2(a)(ii) (requiring that the supervising attorney be identified in the application). The order may, of course, identify more than one supervising attorney.

(c) the identity of the agency employing the law enforcement officers authorized to intercept communications;

Commentary to Standard 2-4.8(c)

This provision is derived from Standard 2-5.8(b) of the Second Edition, which required the order to identify "the agency to which authority to overhear or record or to which approval of overhearing or recording is granted." The changes are stylistic only.

(d) the identity of the person, if known, whose communications are to be intercepted;

Commentary to Standard 2-4.8(d)

This provision is derived from Standard 2-5.8(c) of the Second Edition, which required that the order include "the identity of the person, if known, whose communications are to be or were overheard or recorded." The changes are stylistic only.

(e) a specification of the particular offense as to which electronic surveillance is approved;

Commentary to Standard 2-4.8(e)

This provision is derived from Standard 2-5.8(d) of the Second Edition, which referred to "the particular offense as to which overhearing or recording is authorized or was approved." The changes are stylistic only.
(f) a particular description of the communications sought to be intercepted;

Commentary to Standard 2-4.8(f)

This provision is derived from Standard 2-5.8(e) of the Second Edition, which required an electronic surveillance order to include "a particular description of the communications sought to be or which were overheard or recorded." The changes are stylistic only.

(g) a particular description of the facilities from which or the place where the communications to be intercepted are or will be occurring, unless the order is issued pursuant to Standard 2-4.10;

Commentary to Standard 2-4.8(g)

This provision is derived from Standard 2-5.8(f) of the Second Edition. In addition to stylistic changes, it adds a reference to Standard 2-4.10, which permits the issuance of an order not specifying a facility or place if the applicant demonstrates that "specification of the facilities or place is not practical." See the commentary to that Standard.

(h) a directive that the interception of communications shall begin at a specified time or as soon as practicable, and in any case, no later than ten days after the order is issued;

Commentary to Standard 2-4.8(h)

This provision is derived from Standard 2-5.8(g) of the Second Edition. In addition to making stylistic changes, it adds the requirement that the interception of communications may begin "no later than ten days after the order is issued." The limit of ten days is taken from 18 U.S.C. § 2518(5), which provides, in pertinent part, that an order may authorize electronic surveillance for a maximum of thirty days, and that "[s]uch thirty day period begins on the earlier of the day on which the investigative or law enforcement officer first begins to conduct an interception under the order or ten days after the order is entered." Some limitation on the discretion of the executing officers to begin intercepting communications after the order is issued is appropriate, not least of all because the probable cause underlying the application may grow stale if the delay in execution is too long.
(i) where requested and approved, a directive requiring electronic communication service providers, landlords, custodians, or other persons to furnish information, facilities, or technical assistance, and authorizing compensation for the costs of such assistance;

**Commentary to Standard 2-4.8(i)**

This provision is derived from Standard 2-5.8(h) of the Second Edition, which permitted an electronic surveillance order to include a directive "requiring telephone or telegraph companies, landlords, custodians, or other persons" to furnish such assistance. By making reference to "electronic communication service providers," a term defined by Standard 2-2.1(g) as "person[s] or entity[ies] which, in the ordinary course of business, routinely [provide] a service allowing [their] users to send or receive private communications," the provision, as modified, is not limited to telephone and telegraph companies, but extends to those who furnish other types of electronic communication services. The directive contemplated by this provision may be contained in an order separate from but incorporated in the electronic surveillance order, so that the entity or person served with the directive is not informed, inter alia, of the persons and crimes specified in the order.

(j) a directive that minimization of the intercepted communications be accomplished contemporaneously with their interception;

**Commentary to Standard 2-4.8(j)**

If particularization is the means by which a court limits the scope of the search authorized by an eavesdropping warrant, minimization is the obligation placed upon the law enforcement officers executing the warrant to attempt to limit those communications they intercept to those which the warrant particularly authorizes them to seize. Minimization is thus required in order to make the execution of an electronic surveillance order a reasonable search within the meaning of the Fourth Amendment. Agents executing an eavesdropping warrant fulfill the

---

128. "In light of the [Supreme] Court's condemnation in Berger [v. New York, 388 U.S. 41 (1967)] of completely open-ended surveillance, it was necessary for Title III to include a regulatory mechanism to avoid indiscriminate, unlimited, uncontrolled surveillance. That devise is the requirement that the order contain the minimization directive..." Carr, *The Law of Electronic Surveillance* (2000), at 5-30-5-31.
minimization requirement by intercepting some communications, and some portions of communications, but not others. What techniques or procedures will be most effective at capturing communications relevant to the crime which is the authorized subject of electronic surveillance and at minimizing the interception of those which are not will depend on the facts of each case. Thus it is not surprising that the National Wiretap Commission concluded that minimization requirements are not "susceptible to general statutory definition."129

The minimization techniques employed may be extrinsic or intrinsic to the contents of the communication, or they may be a combination of both. Extrinsic minimization may be based upon such factors as the day of the week or the time of the day. When an order authorizes the interception of telephonic communications, a determination may be made to intercept, or not to intercept calls made or received from particular numbers. When an order authorizes the interception of oral communications, execution of the order may be limited to times when physical surveillance indicates that certain persons are or are not present. Whatever the external parameters may be, a communication not falling within those parameters should not be intercepted at all.

In contrast, intrinsic minimization is employed by initially intercepting a communication, determining who the parties are130 and what the subject of their communication is, and then determining whether or not the communication is pertinent to the investigation or privileged.131 If

---


130. A warrant may authorize the interception only of communications to which at least one of the subjects named in the warrant is a party ("the communications of X, Y, and Z, with their agents, co-conspirators and others as yet unknown"), or it may authorize the interception of any pertinent communications, regardless of whether a named subject is a party to it ("the communications of X, Y, and Z, and their agents, co-conspirators and others as yet unknown"). See United States v. Kahn, 414 U.S. 143 (1974). "Where the interception order restricts the monitors to intercepting conversations in which at least one named suspect is a part, monitors do not have the right to listen to a conversation until they determine whether it is 'pertinent'; they only have the right to listen until they determine whether a named suspect is on the phone." Fishman and McKenna, Wiretapping and Eavesdropping (2d Ed. 2000), at 14-23.11, n. 83 (citations omitted). If, before making that determination, the monitors discover that the communication is criminal, they may arguably continue to intercept it in "plain view" even after learning that none of the parties is named in the order. 1 Carr, The Law of Electronic Surveillance 5-12 (2000).

131. Most courts allow up to two minutes for the intercepting officers to determine the pertinency of a communication, but as patterns of use and users develop over the course of the execution of the order, a shorter time should usually be sufficient. See Carr,
the intercepting officer determines that the communication is not pertinent, he or she ceases to intercept it, at least for a period of time until the communication is "spot monitored" to determine if the subject matter has changed and become relevant. 132

As the Supreme Court has recognized, "the circumstances of the wiretap" may bear on the degree of the minimization required. 133 The nature of the criminal activity is a factor, since if a "widespread conspiracy" is under investigation, more extensive surveillance may be necessary to determine its scope and to intercept its many co-conspirators in incriminating conversations. 134 The nature of the location or facility subject to the eavesdropping is also a factor, since many innocent people may use some locations or facilities, while others may be used more or less consistently for criminal purposes. 135 The length of time the electronic surveillance has been conducted is yet another factor. 136

Standard 2-5.8(i) of the Second Edition requires that an electronic surveillance order contain a directive that overhearing or recording shall be conducted in such a way as to minimize the overhearing or recording of conversations not otherwise subject to overhearing or recording."

The Law of Electronic Surveillance (2000), at 5-39-5-41. Longer periods have been approved, both initially and later, when "speakers use defensive techniques, such as coded language, or other difficulties impede the determination of pertinence." Id. at 5-40.

132. "Spot monitoring, which has been described as 'highly persuasive evidence of a good faith intention on the part of the monitors to minimize,' and which lasts from one to three minutes at intervals of ten to thirty minutes has been approved." I Carr, The Law of Electronic Surveillance (2000), at 5-42 (footnote omitted). "One decision to the contrary notwithstanding, merely turning off a recorder while the monitoring agent continues to listen to the conversation does not satisfy the minimization requirement." Id., at 5-43 (footnotes omitted).


134. Scott v. United States, 436 U.S. 128, 140 (1978). "Courts have been particularly permissive with regard to minimization practices in investigations of complex narcotics conspiracies. However, the goals of the investigation and the scope of criminal activity have been cited as justifying extensive interception in cases involving other types of crime, as well." Fishman and McKenna, Wiretapping and Eavesdropping (2d Ed. 2000), at 14-18-14-19 (footnotes omitted).

135. In Scott, 436 U.S. at 140, for example, the Supreme Court suggested that the amount of minimization required would be greater if agents tapped "a public telephone because one individual is thought to be placing bets over the phone" than if they tapped "a phone located in the residence of a person who is thought to be a head of a major drug ring." See also United States v. Dorfman, 542 F. Supp. 345, 491 (N.D.Ill. 1982), aff'd 690 F.2d 1217 (7th Cir. 1982), and aff'd 737 F.2d 594 (7th Cir. 1984).

136. "During the early stages of the surveillance the agents may be forced to intercept all calls to establish categories of nonpertinent calls which will not be intercepted thereafter. Interception of those same types of calls might be unreasonable later on, how-
Similarly, 18 U.S.C. 2518(5) requires that an eavesdropping warrant provide that "the authorization to intercept . . . shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter. . . ." The present provision more simply requires that an order direct that "minimization of the intercepted communications be accomplished."

When evaluated in light of two definitions included earlier in the Third Edition, the general reference to "minimization" in Standard 2-5.8(i) is, in fact, more precise than the language used both in the Second Edition and in Title III. Standard 2-2.1(d) of the Third Edition defines minimization as "a good faith effort made to limit the interception of communications to those communications, or portions thereof, which are subject to interception pursuant to an electronic surveillance order," and Standard 2-2.1(e) provides that "[a] communication is ‘subject to interception’ if it is intercepted during lawfully conducted surveillance and: (i) it is evidence of an offense which is an authorized subject of the electronic surveillance, or of another offense; and (ii) the communication is not privileged under applicable state law."

In requiring that electronic surveillance orders include a minimization directive, Standard 2-5.8(i) adds the specification that the directive be that the minimization "be accomplished contemporaneously with [the] interception." This additional language was added in light of the exception set forth in Standard 2-5.9 which permits, in certain circumstances, that minimization be accomplished after communications are intercepted, in order to emphasize the contemporaneous interception is required whenever those exceptional circumstances are not present.

The Supreme Court has held that in determining whether to suppress the communications seized during court-ordered electronic surveillance, whether intercepting officers made a "good faith effort" to minimize the interception of non-pertinent communications is only one factor. 137 The Third Edition of the Standards nonetheless defines minimization to require a "good faith effort to limit the interception" of non-

---

137. Scott v. United States, 436 U.S. 128, 140 (1978). In Scott, the Court observed that in determining whether to suppress communications for a failure to minimize adequately, the focus should be on the intercepting officers actions and not their motives. Thus, the Court held that communications intercepted by officers who made no attempt at minimization at all should not have been suppressed because, under the particular circumstances of the case, it was not objectively unreasonable for them to have intercepted all the communications.
pertinent and privileged communications because doing so "exert[s] an additional and useful influence over the execution of electronic searches."\(^{138}\)

**(k)** a statement of the maximum period of authorized electronic surveillance, which shall not be longer than warranted by the showings of probable cause required by subdivisions (a) and (b) of Standard 2-4.3, and in any event, not longer than thirty days from the time specified for the beginning of interception of communications;

**Commentary to Standard 2-4.8(k)**

Standard 2-5.8(j) of the Second Edition provided that an electronic surveillance order should contain "a statement of the maximum period of overhearing or recording, which shall not be longer than necessary to accomplish the objective of the overhearing or recording warranted by the showing of probable cause under Standard 2-5.4(a)(i) and, in any event, not longer than fifteen days from the time specified for the beginning of the overhearing or recording." Standard 2-4.8(k) makes several changes in that formulation.

First, the language requiring that the authorized period "not be longer than necessary to accomplish the objective of the [electronic surveillance]" was omitted, since subdivision (l) of this Standard already requires that an order must include "a directive that interception of the communications shall terminate upon the accomplishment of the objectives of the electronic surveillance ..." The current provision does, however, retain the requirement that the authorized period should "be no longer than warranted by the showings of probable cause required by subdivisions (a) and (b) of Standard 2-4.3."\(^{139}\) If, for example, there is

\(^{138}\) 1 Carr, The Law of Electronic Surveillance (2000), at 5-47. Judge Carr notes that "some states, including New Jersey and New York, have rejected the Supreme Court's approach in Scott and have imposed a good faith standard." Id.

\(^{139}\) Standard 2-4.3(a) requires that the application establish probable cause to believe that "a person is committing, has committed, or is about to commit a particular designated offense." Standard 2-4.3(b) requires that the application establish probable cause to believe that "evidence concerning that particular offense may be obtained through the electronic surveillance" sought. The probable cause showing required by Standard 2-5.4(a)(i) of the Second Edition for an "extended period of electronic surveillance"—that "the person is presently or was then engaged over a period of time in the commission of a particular offense with three or more close associates as part of a continuing criminal activity"—has been eliminated in the Third Edition. See the commentary to Standard 2-4.3(a).
probable cause that communications relating to the crime which is the subject of the surveillance will occur for only a few days, authorizing electronic surveillance for a longer period would not be justified.

Although the Second Edition of the Standards, like the First, limited the maximum authorized period for an electronic surveillance order to fifteen days, the Third Edition has increased it to thirty. This change was made to conform the Standards to Title III, which likewise make the maximum authorized period of surveillance thirty days. 18 U.S.C. 2518(5). This change is not intended to create a presumption that the authorized period of an order should be thirty days; as before, the period should be no longer than the probable cause showing in the application justifies. Furthermore, Standard 2-4.6(b)(i) specifically provides that a judge who issues an electronic surveillance has discretion to reduce the authorized period from that requested in the application. In any case, as already noted, subdivision (1) of this Standard requires that, regardless of the maximum period specified in the order, authorization must end if the objectives of the surveillance are accomplished earlier.

(l) a directive that the interception of communications shall terminate upon the accomplishment of the objectives of the electronic surveillance, as those objectives are set forth in the application pursuant to Standard 2-4.2(a)(vi), and are approved by the court; and

Commentary to Standard 2-4.8(l)

This provision is derived from Standard 2-5.8(k) of the Second Edition, which required that an electronic surveillance order contain "a directive that the overhearing or recording shall terminate upon the accomplishment of its objective." Beyond the stylistic changes, Standard 2-4.8(l) adds a reference to the requirement in Standard 2-4.2(a)(vi) that the application for an electronic surveillance order set forth the objectives of the electronic surveillance sought. As amended, this provision also implements the general principle set forth in Standard 2-3.1(c)(i)(C) that an electronic surveillance order should only issue when "the judge issuing the order approves the objectives of the electronic surveillance . . ." As set forth in the commentary to that general principle, in considering whether to approve those objectives, the appropriate inquiry for the judge is: are the objectives of the investigation directed toward the prosecution of the crimes which are the subject of the electronic surveillance order and are those objectives reasonably obtainable?
(m) a directive that the prosecuting attorney the application states will supervise the execution of the order, or another prosecuting attorney acting on his or her behalf, must supervise the execution of the order, and, unless the authorized period of electronic surveillance is ten days or less, periodically submit progress reports to the court containing:

(i) information reasonably adequate to permit the judge to review whether the order is being executed in a manner which minimizes the interception of communications not otherwise subject to interception, and whether continued interception of the communications pursuant to the order is necessary to achieve the objectives of the electronic surveillance, as those objectives are set forth in the application pursuant to Standard 2-4.2(a)(vi) and approved by the court pursuant to Standard 2-4.8(l);

(ii) notice of the interception and content of any communication, if known, that does not relate to an offense specified in the electronic surveillance order, but does relate to another offense not specified in that order, and

(iii) identification, by number or otherwise, of the records made of the contents of the intercepted communications pursuant to Standard 2-4.14.

Commentary to Standard 2-4.8(m)

Standard 2-5.8(1) of the Second Edition of the Standards provided that an electronic surveillance order should contain "a directive, where appropriate, that progress reports shall be submitted periodically to the court." Standard 2-4.8(m) of the Third Edition adds to this provision a requirement that the directive require that the electronic surveillance be supervised by the prosecuting attorney specified for that purpose in the application, or by another prosecuting attorney acting on his or her behalf, and makes the supervising attorney (or the attorney acting on his or her behalf) specifically responsible for the submission of the progress reports. Title III permits a judge to require the submission of progress reports, but does not mandate that the judge do so. See 18 U.S.C. § 2518(6). Although Standard 2-5.8(l) of the Second Edition stated that progress reports should be required only "where appropriate," the commentary to that provision described the reports as being "mandatory rather than discretionary. ..." The present version makes clear that progress reports are mandatory "unless the authorized period of surveillance is ten days or less."
While the earlier editions of the Standards did not specify what information a progress report should contain, Standard 2-4.8(m) does. The information required is that necessary for the role assigned to the judge by the general principle set forth in Standard 2-3.1(c)(iii): to "ensure that [the electronic surveillance order] is executed appropriately." A judge can meaningfully carry out this function only if, during the course of the authorized period of electronic surveillance, the judge is regularly and routinely provided with sufficient information concerning the communications intercepted. Thus, subdivision (i) of Standard 2-4.8(m) requires that progress reports contain "information reasonably adequate to permit the judge to review whether the order is being executed in a manner which minimized the interception of communications not otherwise subject to interception and whether continued interception of the communications pursuant to the order is necessary to achieve the objectives of the electronic surveillance" as those objectives were approved by the court in issuing the order.

"Plant reports" prepared by the intercepting officers are useful for this purpose (as are reports now automatically generated by some electronic surveillance equipment) which document when the interception of each communication begins and ends, and for how long the interceptions last. "Plant reports" also typically include brief summaries of intercepted communications, and more extensive summaries, and even transcripts, of portions of significant communications should also be included in progress reports, as should affidavits from the supervising attorney detailing the minimization instructions given to the intercepting officers and any special minimization problems that have arisen and how they were resolved. When provided with a progress report, the judge

140. The commentary to Standard 2-5.8(l) of the Second Edition explains that "[n]o specific form or substance [for progress reports] is mandated by the standard, as different circumstances in particular cases will require flexibility." 18 U.S.C. § 2518(6) describes the reports a judge may require as "showing what progress has been made toward the authorized achievement of the objective and the need for continued interception," but also does not specify the form such reports should take. "In the absence of statutory specifications, it has been held that their form is discretionary with the judge, and that written reports are not required under § 2518(6)." 1 Carr, The Law of Electronic Surveillance (2000), at 5-63 (footnote omitted).

141. Judge Carr recommends that "[a]t a minimum, the reporting officers should provide the court with summaries of pertinent calls, details about the total number of calls intercepted on a day-by-day basis, the number of calls actually completed, the number of calls over two minutes in length, and the number of calls minimized. Forms should be developed and completed, and narrative or verbatim portions of intercepted calls presented whenever possible." 1 Carr, The Law of Electronic Surveillance (2000), at 5-64 (footnote omitted).
may, of course, require that further information be provided, and should point out any concerns arising from the information, give guidance and/or instructions concerning the minimization process, and determine whether the surveillance should continue or terminate.

In lieu of requiring that an application be made for an order approving the "plain view" interception of a communication relating to a crime which is not the authorized subject of electronic surveillance order [see the commentary to Standard 2-4.5], subdivision (ii) of Standard 2-4.8(m) requires that the progress report provide "notice of the interception and content of any communication, if known, that does not relate to an offense specified in the electronic surveillance order, but does relate to another offense not specified in the order." Armed with this information, the judge can determine whether the communication was properly intercepted, and provide guidance and/or instructions to the supervising attorney concerning the interception of any such communications in the future execution of the order. For purposes of this provision, a communication is "known" to relate to an offense not specified in an electronic surveillance order if there is probable cause to believe such an offense has been, is being, or is about to be committed, and that the communication relates to that offense.142 This provision does not require notice of the interception of communications which relate both to an offense specified in the electronic surveillance order and another offense, since such an interception is specifically authorized by the order.

Subdivision (iii) of Section 2-4.8(m) requires that the progress report also include information containing "identification, by number or otherwise, of the records made of the contents of the intercepted communications pursuant to Standard 2-4.14." While the obligation that recordings of intercepted tapes be sealed before the judge was intended to protect their integrity, that procedure also satisfied the requirement of furnishing a return on the judge's order, a requirement the Supreme Court has suggested is constitutionally necessary.143 Although the Third

---

142. See United States v. Kahn, 415 U.S. 143 (1974) (requirement in 18 U.S.C. § 2518(4)(a) that electronic surveillance order identify "the person, if known, whose communications are to be intercepted" means all persons there is probable cause to believe are committing crimes specified in the order and will be intercepted in its execution).

143. See Berger v. New York, 388 U.S. 41, 60 (1967) (finding New York's electronic surveillance statute defective because, inter alia "the statute [does not] provide for a return on the warrant thereby leaving full discretion in the officer as to the use of seized conversations of innocent as well as guilty parties").
Edition of the Standards no longer requires judicial sealing [see the commentary to Standard 2-4.14], requiring that progress reports identify for the judge those records made of the intercepted communications replaces the requirement that the executing officers make a "return" on the electronic surveillance order, and provides the judge with the opportunity to make provision for the custody of the records and for the use of the communications included in or on them. For this purpose, a final progress report should be made after electronic surveillance pursuant to the order is terminated.

Like the previous editions of the Standards and Title III, Standard 2-4.8(m) does not specify how often progress reports should be made. The goal in determining their frequency, however, should be to provide the judge with information in a fashion sufficiently timely to permit him or her to monitor the execution of the order and, if necessary, to alter the way it is being executed before errors are unnecessarily repeated and/or the electronic surveillance ends. Standard 2-4.6(b)(iii) authorizes the judge to modify the frequency with which progress reports must be submitted.

**Standard 2-4.9. Minimization after communications intercepted**

(a) When it is not reasonably possible to satisfy the minimization requirement of Standard 2-4.8(j), either because the technological means by which the intercepted communications are transmitted do not permit it, or because the intercepted communications are in a code or foreign language which cannot reasonably be deciphered or translated at the time of interception, the minimization requirement set forth in that standard should be considered satisfied if:

(i) a law enforcement officer who is familiar with the investigation of the offense for which the electronic surveillance is authorized, or an individual acting under the supervision of such a law enforcement officer, accomplishes that minimization as soon as practicable after the communications are intercepted;

---

144. "Justice Department policy requires submission of progress reports at five-day intervals." Carr, *The Law of Electronic Surveillance* (2000), at 5-62. For an order authorizing electronic surveillance for thirty days, progress reports should be required, at a bare minimum, no less often than every ten days.
Commentary to Standard 2-4.9(a)(i)

Standard 2-4.8(j) requires that an electronic surveillance order contain "a directive that minimization of the intercepted communications be accomplished contemporaneously with their interception. In some cases, however, such "real time" minimization may be not possible because the communications are conversations spoken in a foreign language and intercepting officers fluent in that language are not reasonably available. In other cases—for example, the interception of electronic mail, a facsimile transmission (or "fax"), or the transmission of data from one computer to another by modem—contemporaneous interception may not be technologically possible, because the communication can be intercepted only in its entirety or not at all, and its contents can be examined only after interception of the entire communication is completed. In both kinds of situations, minimization after interception is all that is possible.

The First and Second Edition of the Standards include no provision for such "after-the-fact" minimization, nor did Title III when it was first enacted. However, in the Electronic Communications Privacy Act of 1986, Congress specifically provided that "[i]n the event the intercepted communication is in a code or foreign language, and an expert in that foreign language or code is not reasonably available during the interception period, minimization may be accomplished as soon as practicable after such interception." 18 U.S.C. 2518(5). While Title III was not explicitly amended to permit after-the-fact minimization for electronic communications, the Senate Report for ECPA recognized that "real time" minimization was not always possible when intercepting such communications, and specifically expressed its intent that when it was not, minimization could be conducted after their interception.145

145. "The Committee recognizes that although the statutory standards for minimizing wire, oral and electronic communications are the same under proposed subsection 2518(5), the technology used to either transmit or intercept an electronic message such as electronic mail or a computer data transmission ordinarily will not make it possible to shut down the interception and taping or recording equipment simultaneously in order to minimize in the same manner as with a wire interception. It is impossible to 'listen' to a computer and determine when to stop listening and minimize as it is possible to do in listening to a telephone conversation. . . . Thus, minimization for computer transmissions would require a somewhat different procedure than that used to minimize a telephone call. Common sense would dictate, and it is the Committee's intention, that the minimization should be conducted by the initial law enforcement officials who review the transcript. Those officials would delete all non-relevant materials and disseminate to other officials only that information which is relevant to the investigation." Senate Report 99-541, 99th Cong., 2d Sess., 1986 U.S. Code Cong. & Admin. News 3555, 3585.
Standard 2-4.9(a) provides “black letter” authorization for minimizing communications after their interception, not only for coded and foreign language communications, but also for those in which technology is the barrier to contemporaneous minimization. This provision follows federal law in requiring that such minimization be accomplished “as soon as practicable” after the communications are intercepted.

Standard 2-4.9(a) permits after-the-fact minimization only “when it is not reasonably possible to satisfy the [contemporaneous] minimization requirement of Standard 2-4.8(j), either because the technological means by which the intercepted communications are transmitted do not permit it, or because the intercepted communications are in a code or foreign language which cannot reasonably be deciphered or translated at the time of interception.” While technology generally makes contemporaneous minimization of electronic communications downright impossible, a determination of when it is “not reasonably possible” to contemporaneously minimize communications in a foreign language must necessarily be more fluid.146 If, for example, the language is Spanish, and the electronic surveillance is being conducted by an agency in a large urban area, officers fluent in Spanish are usually “reasonably” available. On the other hand, in a smaller community, or for communications in a less common language or dialect, there may be no officers capable of translating the communications, either in the law enforcement agency conducting the surveillance, or in any agency nearby.147

146. See 1 Carr, The Law of Electronic Surveillance (2000), at 5-54 (“An initial question, where foreign language conversation[s] have not been minimized, is whether the officers reasonably should have foreseen that intercepted conversations would not be in English. If the failure to anticipate foreign-language conversations was reasonable, the minimization inquiry will focus on whether the agents diligently sought to obtain a translator to monitor the conversations as they were occurring or after interception to provide prompt post-hoc minimization.”) (footnotes omitted).

147. Note that the definition of a law enforcement officer includes “any agent of such officer,” 2-2.1(f). Thus, just as 18 U.S.C. §2518(5) permits interception of communications “by an individual operating under contract with the Government, acting under the supervision of an investigative or law enforcement officer authorized to conduct the interception,” so, under the Standards, may an “agent” of a law enforcement officer, acting under his or her supervision, conduct minimization of communications contemporaneously with their interception, or after they are intercepted. Particularly if the agent is a person (like an instructor or student in the foreign language at a nearby university) who has no previous experience in law enforcement, it may not be sensible to allow him or her to actually intercept communications, and the number of available agents proficient in a particular language or dialect might, in any case, be insufficient to permit them to do so given the authorized period of interception.

137
Moreover, officers fluent in a particular language may not "reasonably" be available at the inception of surveillance, but may become available thereafter.\footnote{See, e.g., United States v. David, 940 F.2d 722, 730 (1st Cir. 1991), in which, more than two weeks after an electronic surveillance order issued, Israeli police officers began to be employed "as interpreters capable of understanding modern Hebrew as it pertained to drug dealings." Until then, Hebrew conversations were intercepted in full and minimized after the fact. The Court held that "this schedule comported with the statutory directive. The government need not show, as a prerequisite to after-the-fact minimization, that contemporaneous minimization was an utter impossibility. Here, the evidence indicated that, despite reasonable, good-faith efforts, Hebrew interpreters were not available at all times." Id.}

While, at first blush, it might seem desirable to have after-the-fact minimization conducted by someone totally removed from the investigation, only "a law enforcement officer who is familiar with the investigation of the offense for which the electronic surveillance is authorized" has the knowledge necessary to minimize appropriately, since only an officer who is so informed can sort out the pertinent communications from the non-pertinent ones. Indeed, the officer must receive information concerning not only the ongoing electronic surveillance but all other aspects of the continuing investigation as well. Only then can the officer keep abreast of all of the identified subjects of the electronic communications and the kinds of criminal communications they are likely to be having. And only then can the officer stay informed of those persons who had been identified as playing no role in the crimes that were the subject of the electronic surveillance, and whose communications were not likely to be pertinent to those crimes.

(ii) to the extent reasonable and possible, that minimization is accomplished in a manner designed to protect the privacy interests of the parties to the communications to the same extent as properly conducted contemporaneous minimization, had contemporaneous minimization been possible;

Commentary to Standard 2-4.9(a)(ii)

An officer who conducts minimization after-the-fact might do so by reading or listening to the communication in its entirety, and then disclosing to those officers conducting the investigation all of the pertinent parts of the communication (as well as any parts relating to crimes not
specified in the electronic surveillance order). Such a process would arguably give the minimizing officer the maximum degree of accuracy in sifting out the pertinent communications from the non-pertinent ones, thus best guaranteeing that all criminal communications, but no innocent ones, were disseminated to the officers conducting the investigation. This may, indeed, be the process contemplated by Congress.\textsuperscript{149} It is the judgement of the Standards, however, that this approach intrudes on privacy, rather than protects it, because it permits the intercepting officer to read or listen to every intercepted communication, and every portion of every intercepted communications, simply because it was "not reasonably possible" to intercept less than everything. Thus, Standard 2-4.9(a)(ii) requires that after-the-fact minimization be accomplished "to the extent reasonable and possible . . . in a manner designed to protect the privacy interests of the parties to the communications to the same extent as properly conducted contemporaneous minimization, had such minimization been possible."\textsuperscript{150}

For the interception of communications in a foreign language, the implementation of this requirement is reasonably straightforward since, as occurred in \textit{United States v. David}, a "protocol" can be "designed to replicate what would happen in a contemporaneous minimization: the interpreters [can] be told to stop listening to a tape once they determined that the conversation was beyond the scope of the investigation."\textsuperscript{151} With greater difficulty, the minimization of electronic communications can also be accomplished by a protocol that attempts to "replicate" contemporaneous minimization. As with contemporaneous minimization, the offi-

\textsuperscript{149} "[M]inimization should be conducted by the initial law enforcement officials who review the transcript. Those officials would delete all non-relevant materials and disseminate to other officials only that information which is relevant to the investigation." Senate Report No. 99-541, 99th Cong., 2d Sess., 1986 U.S. Code Cong. \& Admin. News 3555, 3585.


\textsuperscript{151} 940 F.2d 722, 730 (1st Cir. 1991). Recording all that they listen to, as they listen to it, the interpreters can disseminate to those conducting the investigation only the communications as they were minimized, see Standard 2-4.9(iii), and the recording the interpreter creates can be the basis for a future determination as to whether the minimization was proper.
Electronic Surveillance of Private Communications

cer could use both extrinsic and intrinsic minimization methods. Minimizing extrinsically, the officer would consider the identity of the sender and the recipient, in order to determine whether either was specified in the order as a subject of the electronic surveillance. Minimizing intrinsically, the officer would begin reading each communication and would cease to read it if the subject matter appeared not to be pertinent, or became so. For communications of sufficient length, the officer could then "spot monitor" by skipping ahead some reasonable number of lines or pages.

When, however, an officer minimizes non-aural electronic communications by examining every one that is intercepted, problems arise in verifying that minimization was properly conducted. While devices can automatically record whatever an intercepting officer listens to, and prevent the officer from listening without recording, no comparable device can establish that an officer who examined the contents of non-aural communications (on a computer screen, or on a piece of paper, after the contents were printed out) read some but not all of the non-aural electronic communications, or portions of an individual communication but not all of it. Technology, however, can provide an alternative. For example, before each communication is read, an electronic search can be conducted of the intercepted communication for key words or phrases, and the minimizing officer can be limited to opening and reading only those communications containing those words or phrases. If the initial search yields no communications, or only a few, the search can be repeated using other words or phrases—not only once, but many times—without disclosing to the officer the contents of the communications. While those who later reviewed the process would still have only the officer’s word as to which and what portion of the opened communications the officer read, an electronic record could establish which communications were opened, and which were not.

(iii) the minimizing officer, or the individual acting under his supervision, makes at least one original record of the commu-

152. Concerning these methods of minimization, see the commentary to Standard 2-4-8(j).

153. For electronic communications, however, party identification may be less useful than for telephonic ones, since there can be no guarantee that a communication being transmitted via a particular communication service account is being sent or received by the account holder, nor that a party is accurately identified in the communication itself.
tions that the officer determines were otherwise subject to interception, for disclosure to and use by the other law enforcement officers participating in the investigation;

Commentary to Standard 2-4.9(a)(iii)

Subdivision (iii) of Standard 2-4.9(a) authorizes the minimizing officer, or an individual acting under his or her supervision, to disseminate to the other officers participating in the investigation one or more records of those communications "that the officer determines were otherwise subject to interception." Standard 2-2.1(e) provides that "[a] communication is 'subject to interception' if it is intercepted during lawfully conducted electronic surveillance and: (i) it is evidence of an offense which is an authorized subject of the electronic surveillance, or of another offense; and (ii) the communication is not privileged under applicable state law." Pursuant to Standard 2-4.5(a), communications that relate to offenses other than those specified in an electronic surveillance order may be disclosed and used for proper law enforcement purposes, and may be introduced into evidence, if they are intercepted "during lawfully conducted electronic surveillance." Thus, communications relating to other offenses can be used when they are intercepted in plain view by officers who are searching for communications relating to those offenses which are specified in the order. See the commentary to Standard 2-4.5(a). Similarly, when an officer who is conducting minimization after-the-fact finds communications in plain view that relate to other offenses, he may also disclose them to the other officers conducting the investigation. 154

(iv) the minimizing officer preserves an original record of the communications made as they were intercepted and before they were minimized, along with any other original or duplicate of the

154. The argument might be made that because officers who conduct minimization after-the-fact see or hear communications they would not have seen or heard had they minimized contemporaneously, communications they find relating to other crimes are not in plain view. See Downes, "Electronic Communications and the Plain View Exception: More 'Bad Physics,'" 7 Harv. J. Law & Technology 239, 276 (1994). Whatever the validity of this argument, however, it is applicable only when the minimizing officer reads or listens to all of the intercepted communications, and not when, as Standard 2-4.9(ii) requires, minimization after-the-fact "is accomplished in a manner designed to protect the privacy interests of the parties to the communications to the same extent as properly conducted minimization. . . ."
record used to accomplish the minimization, using procedures designed
to prevent others from having access to the contents of the record; and
(v) the contents of the communications that the minimizing officer
determines were not otherwise subject to interception are not
otherwise disclosed, except as authorized by judicial order.

Commentary to Standard 2-4.9(a)(iv) and (v)

The purpose of minimization after-the-fact would be frustrated, and
the reasonableness of the search conducted by the minimized officer
negated, if, after the minimization was accomplished, the communica-
tions the minimizing officer determined were not "otherwise subject to
interception" were then disseminated to the other law enforcement offi-
cers participating in the investigation. Thus, subdivision (iv) of Standard
2-4.9(a) requires the use of "procedures designed to prevent others from
having access to the contents of the record" made of the intercepted but
unminimized communications, and subdivision (v) prohibits the dis-
closure of those communications the minimizing officer determines
were "not otherwise subject to interception "except as authorized by
judicial order." Both provisions are consistent with the suggestion con-
tained in the Senate Report for the Electronic Communications Privacy
Act that when foreign language communications are minimized after they
are intercepted, the minimizing officer should "delete all non-relevant
material and disseminate to other officials only that information which
is relevant to the investigation."155 An exception is made for dissemina-
tion of the contents of such communications "when authorized by court
order" for purposes of Standard 2-6.2(e), which, when after-the-fact min-
imization is conducted, requires the court to disclose to the defendant
"the communications that the minimizing officer determined were not
otherwise subject to interception." For the purpose of requiring this dis-
closure, see the commentary to Standard 2-6.2(e). The exception is not
limited to this purpose, since disclosure may be appropriate for reasons
not contemplated by these Standards. Disclosure for any other purpose,
however, should be ordered only when circumstances are compelling,
and override the privacy interest of the parties to the communications to
be disclosed.

News 3555, 3585.
(b) When the electronic surveillance order does not already authorize such minimization procedures, the judge who issued the order should be notified, in the next progress report or application for an extended electronic surveillance order, whichever is earlier, that such procedures are being employed.

Commentary to Standard 2-4.9(b)

This provision, like others in the Standards, is designed to implement the general principle set forth in Standard 2-3.1(iii), which states that a judge who issues an electronic surveillance order "can and should assure that it is executed appropriately." If the need for after-the-fact minimization is contemplated, it is preferable that the applicant notify the judge before the order is issued and seek authority to utilize the procedure. Note that Standard 2-4.6(b)(v) specifically authorizes the judge to modify a proposed order by "specifying or modifying the manner in which minimization is to be achieved, either contemporaneously with or after the communications are intercepted." If the order does not authorize after-the-fact minimization, and the judge is thereafter notified that it is being employed, the judge can then determine that after-the-fact minimization is not necessary, or specify the process by which it should be accomplished.

(c) Whenever progress reports are filed, and within five days after the end of the authorized period of electronic surveillance, the issuing judge should be presented with the original records of the communications thus far preserved by the minimizing officer pursuant to subdivision (a)(iv), and not yet presented to the judge. Those records should be maintained in a place specified by the judge under such conditions as the judge may order, and that place and those conditions should not be changed except by judicial order.

Commentary to Standard 2-4.9(c)

This provision further implements the requirement that those participating in the investigation not have access to the communications the minimizing officer determines were not otherwise subject to interception, and reinforces the judge's role in ensuring the proper execution of an electronic surveillance order, by requiring that the original records of the intercepted communications, in their un-minimized form, be presented to the judge with each progress report and within five days of the
end of the authorized period of electronic surveillance, so that a judicial determination may be made concerning the place where and the conditions under which the records are maintained.

Standard 2-4.10. Order not specifying place or facilities; application and authorization

An order which does not particularly describe the location of the facilities from which or the place where the communications to be intercepted are or will be occurring, may be issued if:

(a) the order otherwise complies with the requirements of Standard 2-4.8;
(b) the application for the order contains a full and complete statement demonstrating that specification of a facility or place is not practical;
(c) the judge issuing the order finds from the application probable cause to believe that such specification is not practical;
(d) the application identifies one or more persons committing the offense; and
(e) the authorization to intercept communications is limited to the interception of communications of the person or persons so identified.

Commentary to Standard 2-4.10

Although an electronic surveillance order must generally specify the facilities over which, or the place where, communications are to be intercepted, in 1986 Congress amended Title III to permit what has become known as “roving” surveillance. A federal electronic surveillance order may authorize a “roving” bug, that is, it may authorize the interception of oral communications without specifying the place where the communications are to be intercepted, if “the application contains a full and complete statement as to why such specification is not practical and identifies the person committing the offense and whose communications are to be intercepted,” and that “the judge finds that such specification is not practical.” 18 U.S.C. § 2518(11)(a). A federal electronic surveillance order

may authorize a "roving wire," that is it may authorize the interception of wire or electronic communications without specifying the facilities from which the communications are to be intercepted, if "the application identifies the person believed to be committing the offense and whose communications are to be intercepted and the applicant makes a showing that there is probable cause to believe that the person’s actions could have the effect of thwarting interception from a specified facility," if "the judge finds that such a showing has been adequately made." 18 U.S.C. § 2518(11)(b). When an order authorizes either a roving bug or tap, the interception of a communication may "not begin until the facilities from which, or the place where, the communication is to be intercepted is ascertained by the person implementing the interception order." 18 U.S.C. § 2518(12). While the Supreme Court has held that specification of the place or facility is generally necessary to satisfy the requirements of the Fourth Amendment, the courts that have considered the issue have upheld the constitutionality of federal order that include roving authority pursuant to 18 U.S.C. § 2318(11).

157. The list of federal officials who may apply for a "roving bug" is somewhat more limited than the list of those who may apply a conventional order authorizing the interception of oral communications. Compare 18 U.S.C. § 2516(1) and § 2518(11)(a)(i).

158. The list of federal officials who may apply for a "roving wire" is somewhat more limited than the list of those who may apply a conventional order authorizing the interception of wire communications, compare 18 U.S.C. § 2516(1) and §2518(11)(b)(i), and far more restrictive than 18 U.S.c. § 2516(3), which allows "any attorney for the government" to apply for an order authorizing the interception of electronic communications. Until amended in 1998, § 2518(11)(b) required a showing of "a purpose, on the part of that person, to thwart interception by changing facilities." Because of the difficulties in demonstrating the operation of the mind of a proposed subject of roving surveillance, Congress changed the requirement from showing a "purpose" of thwarting interception to demonstrating that the person’s actions could have the "effect" of doing so, and added an additional condition that an order authorizing a roving wire must provide that "the interception is limited to interception only for such time as it is reasonable to presume that the person identified in the application is ... reasonably proximate to the instrument through which such communication will be ... transmitted." 18 U.S.C. § 2518(11)(b)(iv). Even without this language, however, it would be unreasonable for an intercepting officer to conduct roving surveillance of communications transmitted over a facility after it was no longer "reasonable" to presume the subject of the surveillance was "reasonably proximate" to it.

159. See Berger v. United States, 388 U.S. 41, 55-6 (1967).

160. See, e.g., United States v. Jackson, 207 F.3d 910 (7th Cir. 2000); United States v. Gaytan, 74 F.3d 545 (5th Cir. 1996); United States v. Bianco, 998 F.2d 1112 (2d Cir. 1993); United States v. Petti, 973 F.2d 1441(9th Cir. 1992). In Petti, the court reasoned that a
Standard 2-4.10 follows federal law in sanctioning roving bugs and taps, but varies from federal law in several respects. First, while 18 U.S.C. §2518(11) permits roving authority only for federal electronic surveillance orders, the legislative history offers no justification for not permitting state orders to include such authorization when necessary, and there is no reason to believe that the need for such authority is limited to federal investigations. Thus Standard 2-4.10 permits state as well as federal applicants to seek roving authority. Second, the federal statute makes a distinction between roving bugs, which require a showing that “specification of a place is not practical,” and roving taps, which require a showing that “a person’s actions could have the effect
of thwarting interception from a specified facility.” Because the distinction between the two showings is not meaningful, Standard 2-4.10 requires for both kinds of roving surveillance a showing that specification is “not practical.” Third, the federal statute requires that probable cause be demonstrated in making the showing necessary for a roving tap, but specifies no particular quantum of proof for a roving bug. Because it is not sensible to require probable cause for one but not the other, Standard 2-4.10 requires it for both. Like federal law, Standard 2-4.10 requires that the application for roving surveillance identify one or more persons committing the offense that is the subject of the order, and that the authorization be limited to the interception of the person or persons so identified. Standard 2-4.10(e).

Standard 2-4.11. Extensions

Extensions of an order authorizing electronic surveillance should be granted for periods of not longer than thirty days upon filing and approval of an application in accordance with Standards 2-4.1, 2-4.2, 2-4.3, 2-4.4, and, when applicable, 2-4.10. No limit should be placed on the number of extensions that may be granted. In the exercise of sound discretion, an application for such an extension may be denied, or granted as requested or with appropriate modifications, in accordance with Standard 2-4.6.

Commentary to Standard 2-4.11

This Standard is derived from Standard 2-5.9 of the Second Edition, and includes a number of stylistic and conforming modifications. The

163. In cases in which authority for roving surveillance is sought, the intended subject of the surveillance frequently moves from place to place, or facility to facility, to engage in criminal communications. Facts setting forth this conduct will both demonstrate that particularization of place or facility is “not practical” and that the effect of the subject’s actions could thwart interception from a specified place or facility. This is evident from the legislative history of the roving tap and bug provisions, which explain that for roving bugs, “[s]ituations where ordinary specification rules would not be practical would include those where a subject moves from room to room in a hotel to avoid a bug or where a suspect sets up a meeting with another suspect on a beach or a field,” and that for roving taps, an example of a situation meeting the test of a demonstrated purpose of thwarting investigation [as was originally required] “would be an alleged terrorist who went from phone booth to phone booth numerous times to avoid interception.” Senate Report No. 99-541, 99th Cong., 2d Sess., 1986 U.S. Code Cong. & Admin. News 3555, 3586.
last sentence of the present provision, stating that an application for an extension may be denied or granted as requested or with appropriate modifications, emphasized the important role of judicial discretion in deciding not only whether to grant the initial authority to conduct electronic surveillance, but also in extending that authority. Obviously, a court should have no less discretion in granting an extension for an electronic surveillance order than it does in granting the original order. The reference to Standard 2-4.6 incorporates the many suggestions in that Standard of particular ways in which an order proposed by the applicant—in this case a proposed order of extension—might be modified. See the commentary to that Standard.

Standard 5.9 of the First Edition of the Standards had authorized extensions of up to thirty days, but the maximum period was reduced by Standard 2-5.9 of the Second Edition to fifteen. The commentary to that Standard explained that the reduction “reflect[ed] experience under Title III indicating that the average length of actual surveillance has generally been less than thirty days. Furthermore, reduction of the period for an extension underscores the importance of judicial review and supervision for the entire duration of any surveillance.” The present Standard returns the maximum period for an extension to thirty days, thus conforming it to the thirty day maximum authorized by 18 U.S.C. 2518(5). This change was made for several reasons. The “experience under Title III” on which the commentary to Standard 2-5.9 of the Second Edition relied was taken from statistics that appear in the 1976 National Wiretapping Commission Report. More recently, electronic surveillance has often, and with ample justification, been extended for far more than thirty days. In such cases, doubling the number of applications would be burdensome to both applicants and judges. In any case, because the Standards mandate that the judge receive interim reports on the progress of the electronic surveillance, rather than make such reports discretionary, see Standard 2-4.8(m), and because the Standards effectuate judicial oversight of the execution of an electronic surveillance order in a variety of other ways, see e.g., Standard 2-4.9(b), limiting an extension to a maximum of thirty days is unnecessary to assure judicial involvement in the execution of the order.

As in setting thirty days as the maximum authorized period for the initial surveillance order [see Standard 2-4.8(k)], increasing the maximum period for an order of extension is not intended to create a presumption that authority should be extended for thirty days. The period should be no longer than the probable cause showing in the application.
justifies. And, as in issuing the initial order, a judge who issues an order of extension possesses discretion to reduce the authorized period from that requested in the application. [See Standard 2-4.6(b)(i).] Finally, Standard 2-4.8(l), which applies to extensions as well as to initial electronic surveillance orders, requires that, regardless of the maximum period specified in the order, authorization must end if the objectives of the surveillance are accomplished earlier.

Standard 2-4.12. Privileged communications

(a) No order should be permitted authorizing interception of communications over a facility or in a place primarily used by professionals whose communications are privileged under applicable state law, or in a place used primarily for habitation by a husband and wife, unless, in addition to the showings required under Standard 2.4.3, and, where applicable 2-4.10, the applicant establishes probable cause to believe that there is a particular need to conduct such surveillance over that facility or in that place.

(b) No otherwise privileged communication intercepted in accordance with or in violation of these standards should lose its privileged character.

Commentary to Standard 2-4.12

Title III contains no provision comparable to subdivision (a) of this Standard; subdivision (b) is substantially the same as 18 U.S.C. § 2518(4). The present Standard, which is derived from Standard 2-5.10 of the Second Edition, includes stylistic and conforming changes that are meant to have no substantive impact. The reference to Standard 2-4.10 was necessary because a roving tap or bug could target a facility or location for which a showing of "particular need" is required pursuant to this Standard.

In the Second Edition, Standard 2-5.10 required a showing of "special need." The language was changed here to require a "particular need" because the word "special" is less helpful in conveying what is required: a demonstration that electronic surveillance over some other facility or in some other place could not achieve the authorized objectives of the electronic surveillance, and that surveillance of this particular facility or place is required. Note that this showing must be made only when the facility or place is one "primarily used" by the professional, and not to any facility or place the professional might use. Thus, it is required for
applications seeking electronic surveillance of telephones attorneys regularly use to call their clients, but not to surveillance of telephones clients regularly use to call their attorneys.

Pursuant to subdivision (b) of this Standard, "otherwise privileged" communications remain privileged even if they are intercepted. This provision has no application to communications that would be "otherwise privileged" but are not so because of their criminal nature."164

Standard 2-4.13. Orders and applications; custody; destruction

All orders and applications should be maintained in such places as the judge directs. Orders and applications may be destroyed ten years after they are issued, and may be destroyed earlier when the judge so directs. Orders and applications should not be disclosed except as authorized by statute or judicial order.

Commentary to Standard 2-4.13

This Standard is derived from Standard 2-5.11 of the Second Edition, which provided that "[a]ll orders and applications should be maintained for ten years in such places as the judicial officer directs. They should not be disclosed or destroyed except on judicial order." As modified, the Standard permits orders and applications to be destroyed ten years after issue without judicial approval, which, given the passage of time, is unnecessary. The Standard also permits earlier destruction, when ordered by the judge, but does not contemplate routine destruction before ten years have elapsed. An application for early destruction should be granted only upon a particularized showing that the records should not, or need not, be preserved for the presumptive ten year period. Obviously, destruction should not occur, with or without a court order, while cases in which the use of electronic surveillance pursuant to an order and application are still contemplated, pending, or on appeal.


Standard 2-4.14 implements the general policy set forth in Standard 2-3.1(iv) that "[r]ecordings obtained through the non-consensual acqui-

sition of private communications by use of a mechanical, electronic or other device are usually considered, and ought to be, a highly reliable form of evidence. Accordingly, communications thus acquired should be recorded whenever reasonably technologically possible, and an original copy of the recordings should be maintained in a manner designed to protect their integrity.” Standard 2-4.14 is derived from Standard 2-5.12 of the Second Edition.

(a) At least one original record of the contents of any communications intercepted by electronic surveillance should be made contemporaneously with its interception.

Commentary to Standard 2-4.14(a)

This provision has no counterpart in the First or Second Edition of the Standards, and is meant to make explicit the requirement that the record of an intercepted communication be made “contemporaneously” with its interception. By requiring that “[a]t least one original record” be made of the contents of intercepted communications, the provision recognizes that in some instances more than one original may be generated (as when more than one tape recording is attached to an intercepting device, or when intercepted electronic communications are recorded on two hard drives, one of which is preserved for use at trial, and the other of which is used as a “working copy.”

(b) To the extent possible and reasonable given the form of the communications and the available technology, the equipment and techniques used to make the record should:

(i) enable the intercepting officers to make a complete and accurate record of the intercepted communications, and

(ii) either protect an original record from editing or other alteration, or disclose whether that record has been edited or altered.

Commentary to Standard 2-4.14(b)

This provision implements the general principle set forth in Standard 2-3.1 (c)(iv) that “[t]o maximize the reliability of evidence obtained through the interception of private communications, a record of the contents of the communications thus intercepted should, whenever technologically possible, be made and preserved in a manner designed
to protect its integrity.” This provision is derived from Standard 2-5.12 of the Second Edition, which provided that “electronic surveillance techniques . . . should be so employed that a complete, accurate and intelligible record of the communication will be obtained,” that the contents of intercepted communications “should, if possible be recorded on tape or wire or other comparable device,” and that the recording “should be done in such a way as will protect the recording from editing or other alterations.” \(^{165}\)

Subdivision (i) of Standard 2-4.11(b) abandons the use of the language “tape or wire or other device,” and substitutes the more generic term “record,” since the latter term is broader and encompasses the variety of ways in which aural and non-aural communications can be captured and documented. When the human voice is intercepted in the transmission of an “aural” communication, the intercepted communication can be, and simply and conventionally is, preserved on “tape.” In some cases, the interception of an electronic communication can also be recorded on a “tape.” Now, however, both oral and electronic communications can be recorded on a the hard drive of a computer and / or on a floppy or compact disk. Similarly, when a file is transmitted by modem from one computer to another, and the transmission is intercepted by a court order, the intercepted file can be placed on a disk. When the intercepted communication is a facsimile transmission (a “fax”), its contents can be documented by simply printing out a copy of the fax, or, when technology permits, capturing it as a document on computer or disk. Once, when authorization was obtained to intercept communications to a paging device, the intercepting officers could record the contents of the communications only by writing down the alpha-numeric message received by the clone of the pager in their possession. \(^{166}\) Now it is also possible to save such messages electronically.

Tape recorders are capable of malfunctioning, tape recordings can break or be damaged, and officers who intercept messages to a pager

\(^{165}\) Similarly, 18 U.S.C. § 2518(8)(a) requires that “the contents of any wire, oral, or electronic communication intercepted by any means authorized under this chapter shall, if possible, be recorded on tape or wire or other comparable device” and that the recording “shall be done in such a way as will protect the recording from editing or other alterations.”

\(^{166}\) See United States v. Suarez, 906 F.2d 977 (4th Cir. 1990) (excusing officers intercepting electronic communications transmitted to a “clone pager” from satisfying requirement that the communications be recorded because technologically recording them was not technically possible).
can make errors in reproducing them on paper. While computers can also malfunction, and data recorded on hard drives and disks can be lost, there is no question that technology has improved the ability of a law enforcement officer to create a complete and accurate record of the communications the officer intercepts, and creating records using such this technology reduces the risk of human error or deceit. Accordingly, implicit in this provision of the Standards is that law enforcement should employ technological means that, among those reasonably available, best create "a complete and accurate record" of intercepted communications.

Technology is also the key to achieving the goal of subdivision (b) of Standard 2-4.11(b): to make records using equipment and techniques that "either protect an original record from editing or other alteration, or disclose whether that record has been edited or altered." While digitized data is subject to manipulation, ROM (read only memory) or WORM (write once, read many times) technology is available that prevents editing and alteration of an electronic document. When intercepted communications are recorded on the hard drive of a computer or similar device and then transferred to a disk using such technology (or when they are simultaneously recorded on both), the disk may serve as an "original" record of the communications and the memory on the hard drive may be erased and reused. Equipment and techniques that make a record incapable of modification are preferable. The alternative permitted by subdivision (b)—equipment and technology that disclose whether a record has been edited or altered—was not added to suggest that original records should be modified, but rather to require that when equipment is not reasonably available that prevents editing or alteration, equipment and techniques that indicate when a disk or document has been modified can substitute, since the lack of such an indication will verify that the integrity of the record has been maintained.

Subdivision (a) of 18 U.S.C. § 2518(8)(a) provides that "[i]mmediately upon the expiration of the period of the order, or extensions thereof, [the] recordings [of the contents of any intercepted wire, oral or electronic communication] shall be made available to the judge issuing such order and sealed under his directions," and that "[t]he presence of the seal provided for by this subsection, or a satisfactory explanation for the absence thereof, shall be a prerequisite for the use or disclosure of the contents of any wire, oral, or electronic communication or evidence derived therefrom. . . ." The First and Second Edition of the Standards
mirror Title III in requiring judicial "sealing" of intercepted communications. See Standard 2-5.13. The sealing requirement "does not protect Fourth Amendment interests."167 Instead, as the Supreme Court has observed, it "ensure[s] the reliability and integrity of evidence obtained by means of electronic surveillance. The presence or absence of a seal does not in itself establish the integrity of electronic surveillance tapes. Rather, the seal is a means of ensuring that subsequent to its placement on a tape, the Government has no opportunity to tamper with, alter, or edit the conversations that have been recorded."168 The requirement that the tapes be deliverered to the judge for sealing "does not arise as the tapes are being made during the course of the surveillance," and "delivery may not occur for weeks or months after a particular tape or tapes have been made."169 Judge Carr observes that "[n]o policy supports this situation," and that "[a]s written" the requirement is "meaningless and useless."170

Ironically, and despite its ineffectiveness, the courts have enforced the sealing requirement by focusing not on the method by which the sealing is accomplished—for which evidence tape, masking tape, and even scotch tape have been deemed adequate—but instead on the timeliness of the sealing. Thus, the Supreme Court has held that "the seal required by § 2518(8)(a) is not just any seal but a seal that has been obtained immediately upon expiration of the underlying surveillance order."171 A variety of approaches have been taken in determining how quickly the tapes must be sealed after the termination of the authorized period of eavesdropping. At one extreme, Standard 2-5.14 of the Second Edition of the Standards take a comparatively leisurely approach, not even requiring that tapes be sealed immediately, only "as soon as practicable, but not later than thirty days after the termination of the overhearing or recording." At the other extreme, New York's Court of Appeals has interpreted the state statutory provision that tapes be sealed "immediately" to require that, unless the judge who issued the electronic surveillance order permits otherwise, tapes must be sealed no later than the next business day.

169. 1 Carr, The Law of Electronic Surveillance (2000) at 4-93. "Under the statutory scheme of § 2518(8)(a), therefore, tapes may accumulate and be kept in the officers' exclusive and unsupervised control." Id.
following the expiration of each order. The general rule in the federal courts is that a "modest delay" beyond a day or two requires no further inquiry, but the prosecutor must offer a "satisfactory explanation" for a delay that is "substantial or excessive." When there is an unexcused delay in sealing, the exclusion from evidence of the intercepted communications—and the fruits of those communications—"is frequently ordered . . . even if no challenge has been made to the authenticity or accuracy of the recordings."

In sum, judicial sealing fails to ensure the integrity of records, and leads to the arbitrary suppression of tapes that have not been tampered with, but have been "untimely" sealed. Accordingly, while retaining the concern for the integrity of records expressed in the previous editions and in Title III, the Third Edition of the Standards rejects the almost talismanic approach courts have taken to judicial sealing and abolishes the requirement entirely. By directing its attention to the "equipment and techniques" by which the records are made, Standard 2-4.14(b) looks to technology rather than masking tape to protect the integrity of the

172. See, e.g., People v. Gallina, 66 N.Y.2d 52 (1985) (delay of two business days in sealing tapes not excused by inadequate police procedures or by unavailability of issuing justice on business day when other justices were present); People v. Winograd, 68 N.Y.2d 383 (1986) (suppression required because of unexplained failure to contact issuing justice over weekend and failure to seal before another justice when issuing justice unavailable on religious holiday). New York also requires that sealing occur "immediately" after expiration of each order or extension and not, as under federal law, only "immediately" after all authorized eavesdropping is over. People v. Washington, 46 N.Y.2d 116 (1978). Compare United States v. Carson, 969 F.2d 1480 (3d Cir. 1992); United States v. Vasquez, 605 F.2d 1269, 1276 (2d Cir. 1979).

173. 1 Carr, The Law of Electronic Surveillance (2000), at 5-98–5-99. "The Second and Ninth Circuits have ruled that any presentation of the tapes to the issuing judge more than two days after the end of a wiretap could not be considered 'immediate.' The Third Circuit interprets 'immediately' to mean 'as soon as was practical' and not instanter." The D.C. Circuit has held that a delay of four days requires an explanation.” Fishman & McKenna, Wiretapping and Eavesdropping (2d Ed. 2000), at 16-6 (footnotes omitted).

174. 1 Carr, The Law of Electronic Surveillance (2000), at 5-93 (footnote omitted). An open question exists as to whether or not the statutory requirement of immediate sealing, and the remedy of suppression for untimely sealing, applies to the rescaling of tapes that were lawfully unsealed. See United States v. Vario, 943 F.2d 236 (2d Cir. 1991) (declining to decide question given district court's determination that delays of approximately twenty-eight days in rescaling were satisfactorily explained). But see People v. Sher, 38 N.Y.2d 600 (1976) (suppression of tapes required because of failure of prosecutor to obtain judicial approval to unseal tapes for preparation for and use at trial, and the absence of judicial supervision over the unsealing procedure).
records generated during electronic surveillance. Before they are admitted into evidence, a defendant can challenge the integrity of the records, but the issue for the court and jury should be the same as it is for the integrity of any other kind of physical evidence, to be decided based on the relevant facts, and not on whether an arbitrary and meaningless "sealing" deadline was met.\footnote{See, e.g., United States v. Long, 917 F.2d 691, 700 (2d Cir. 1990) (holding that, on remand, district court should hold evidentiary hearing regarding chain of custody and integrity of tapes that were properly sealed but were subsequently unsealed for an earlier trial); United States v. Angiulo, 847 F.2d 956, 978 (1st Cir. 1988) (finding that when tapes were temporarily unsealed for enhancement, the integrity of the tapes was not compromised).}

Standard 2-5.13 of the Second Edition included, in addition to judicial sealing, a requirement that "a return of the order . . . be made to the judicial officer." This requirement would be satisfied by making the recordings available to the judge for sealing. In place of this "return," Standard 2-4.8(m)(iii) requires that progress reports be given to the issuing judge, not only informing the judge of the progress that has been made toward achieving the results of the electronic surveillance, but also including the "identification, by number or otherwise, of the records made of the contents of the intercepted communications . . . ." See the commentary to Standard 2-4.8(m).

Standard 2-5.13 of the Second Edition also included a provision requiring that after sealing, "the recordings should be maintained in such places and in such custody as the judicial officer directs for at least ten years and should not be destroyed except on judicial order." This provision has been omitted from the Third Edition. The integrity of the records made of the contents of intercepted communications is best protected by the technology with which those records are made. As already noted, if their integrity is called into question, the issue can be litigated. Requiring the judge to supervise the custody of the records is no more likely to afford them additional protection than does requiring them to be sealed under judicial supervision. Moreover, there is no reason why records of the contents of intercepted communications should be preserved any longer than other forms of evidence. Indeed, given the greater privacy interest in intercepted private communications, it could well be argued that when they are no longer needed for purposes of pending litigation, records of the contents of such communications should be destroyed, if anything, earlier than other evidence would
be. Similarly, there is no reason to subject the destruction of such records, but not other kinds of evidence, to judicial supervision.

(c) If such equipment and techniques are used, but fail to make an original record of a particular communication, the law enforcement officer intercepting the communication should transcribe the communication as accurately as possible, and the issuing judge should be notified of the failure and provided with a copy of the transcript no later than the next progress report, or within five days of the end of the authorized period of eavesdropping.

Commentary to Standard 2-4.14(c)

This provision has no counterpart in the First or Second Edition of the Standards. Standard 2-5.12 of the Second Edition did, however, provide that the contents of intercepted communications "should, if possible, be recorded on tape or wire or other comparable device," and 18 U.S.C. § 2518(8)(a) contains almost identical language. The courts have specifically excused a failure to record when it has resulted from a malfunction of the recording equipment. This provision merely sets forth a procedure for such an eventuality and, consistent with the intent of the Standards to effectuate judicial oversight over the execution of electronic surveillance orders, requires that the judge be promptly notified of the malfunction and be provided with a copy of the transcript.

(d) When communications are minimized contemporaneously with their interception, an intercepting officer should take steps to preserve one original record of the intercepted communications immediately after the record is completed, following procedures designed to protect it from editing or alteration.

(e) When communications are minimized after they are intercepted pursuant to Standard 2-4.9, in addition to preserving, as required by Standard 2-4.9(a)(iv), an original record of the communications made as they were intercepted and before they were minimized, the minimizing officer should also take steps to preserve one original record of the minimized communications made pursuant to Standard 2-4.9(a)(iii) immediately after the minimization is accomplished, following procedures designed to protect the record from editing or alteration.

Commentary to Standard 2-4.14(d) and (e)

These subdivisions have no counterpart in the First or Second Edition of the Standards. Both take note of the fact that when records are made of intercepted communications, more than one "original" record may be generated. While privacy requires that care be taken with the custody of all "originals" and any copies made from them, only one original need be preserved for purposes of maintaining an accurate record of the contents of the intercepted communications for disclosure to the defendant, for pre-trial litigation, and for use at trial. As in the making of the record, preservation should be accomplished "following procedures designed to protect the record from editing or alteration." The stringency of the procedure necessary for that purpose will depend on the degree to which the record is susceptible to modification. If the technology of its manufacture is such that it cannot be modified, no special measures will be required.

Subdivision (e) is applicable when communications are minimized after they are intercepted pursuant to Standard 2-4.9. See the commentary to that Standard. When minimization is accomplished after-the-fact, two "original" records must be maintained: one of all the intercepted communications, and another of only those communications, or portions thereof, the minimizing officer determines were subject to interception and discloses to the other officers conducting the investigation.

(f) Under appropriate safeguards, other copies of those records, whether original or duplicate, may be made, used and disclosed for investigative purposes or trial preparation.

Commentary to Standard 2-4.14(f)

This subdivision is taken from Standard 2-5.13 of the Second Edition, which provided that despite the requirement that the recordings of intercepted communications be sealed, "duplicate recordings may be made for use or disclosure for investigative purposes or trial preparation under appropriate safeguards." See also 18 U.S.C. § 2518 (8)(a). The language "whether original or duplicate" was added in recognition of the fact that when records are made of intercepted communications, more than one "original" may be generated, but only one need be preserved for evidentiary use. See the commentary to Standard 2-4.11(e) above.
Standard 2-4.15. Inventory; contents; time; postponement

(a) After the authorization for electronic surveillance, including any extension of that authorization, has ended, the judge should order that an inventory be served on:

(i) the persons named in the order of authorization, and
(ii) any other identified parties to the intercepted communications whom the judge determines should be served in the interest of justice.

(b) The inventory should include notice of:

(i) the entry of the order;
(ii) the date of the entry of the order;
(iii) the period of authorized electronic surveillance;
(iv) the interception, if any, of communications; and
(v) the period, if any, of actual interception of communications.

(c) The judge should order that the inventory be served as soon as practicable, and no later than a specified date, not less than thirty days and not more than ninety days after the authorization for electronic surveillance, including any extension of that authorization, has ended. Upon a showing of good cause made to the judge, the date should be postponed.

(d) Upon application of a person who has received such an inventory, and on notice to the applicant for the electronic surveillance order, the judge may order further disclosure if the judge finds such disclosure is required in the interest of justice.

Commentary to Standard 2-4.15

This Standard is derived from Standard 2-5.14 of the Second Edition.

Subdivision (a) requires the judge to order that inventory notice be served on those named in the order of authorization, and those whom the judge determines should be served "in the interest of justice." If any person not named in the order has been intercepted in inculpatory communications, the interest of justice would generally dictate that they be served with inventory notice, unquestionably so if the prosecuting attorney expects that the person will be prosecuted. The prosecuting attorney who supervised the execution of the electronic surveillance order should furnish the judge with the information necessary to determine who
Electronic Surveillance of Private Communications

should be served, and who need not be.\textsuperscript{177} As the Supreme Court has observed, "while precise identification of each party to an intercepted communication is not required, a description of the general class, or classes, which they comprise is essential to enable the judge to determine whether additional information is necessary for a proper evaluation of the interests of the various parties."\textsuperscript{178} Based on the information supplied, the judge should then issue an order directing that inventory notice be served on particular persons, and need not be served on others, specifying those persons either by name or by class or classes.

While it has been substantially restructured, the restructuring, and most of the changes in language, are stylistic only. Standard 2-5.14 required that inventory notice be served "not later than ninety days after the return is made to the judicial officer . . . ," unless postponed for good cause. Because the Third Edition of the Standards has abolished the requirement for judicial sealing, and provided that the return be made to the judge in a different way, see the commentary to Standard 2-4.14(b), Standard 2-4.14 requires instead that, if not postponed, notice must be served "not more than ninety days after the authorization for electronic surveillance, including any extension of that authorization, has ended." Given that Standard 2-5.13 of the Second Edition required that the return be made "[a]s soon as practicable but not later than thirty days" after the termination of electronic surveillance, this change has the effect of advancing the date from which the timeliness of inventory notice must be measured.

The present Standard adds to the ninety day maximum the requirement that service be made "no less than thirty days" after the end of the authorization. While in many cases, legitimate reasons exist to delay notice for much longer than ninety days, the thirty day minimum was added to discourage the assumption that, as a routine matter, ninety days is "as soon as practicable." The Standard contemplates that the determination of when notice must be served will be made by the judge, who should consult with the attorney who supervised the electronic sur-

\textsuperscript{177} In deciding whether legitimate privacy interests justify withholding inventory notice from parties to intercepted conversations, a judge is likely to require information and assistance beyond that contained in the application papers and the recordings of the intercepted conversations made available by law enforcement authorities.” United States v. Donovan, 429 U.S. 413, 430 (1977).

surveillance concerning when such service is practicable. Authorizing service within ninety days is sensible if it is apparent from the outset that requiring that it occur earlier will result in an application that notice be postponed. Delay beyond the ninety day maximum requires a showing of "good cause."

While Title III requires that inventory notice include the period of authorized surveillance, it does not require "the period, if any of actual interception of communications." See 18 U.S.C. § 2518(8)(d). Standard 2-5.14 of the Second Edition of the Standards required that the inventory report contain this additional information, and the Third Edition retains this requirement.

Both 18 U.S.C. § 2518(8)(d) and Standard 2-5.14 of the Second Edition require that inventory notice be served not only when court authorized electronic surveillance is conducted, but also when, in an emergency situation, communications are intercepted without an electronic surveillance order and an application is made to approve their interception. Under both provisions, service must be made whether the application for approval is granted or denied. For stylistic reasons, the Third Edition of the Standards contains no reference to emergency surveillance outside of Standard 2-5.2, which sets forth when it may be employed, the procedure for making application for approving it after it has occurred, and related matters. If the emergency surveillance is approved, and continuing surveillance authorized, Standard 2-4.15 explicitly requires that inventory notice be served within the requisite period after the authorization ends. Despite the omission of any reference to emergency surveillance in Standard 2-4.15, it should be read to require that, if no additional surveillance is authorized beyond the emergency surveillance, and whether the emergency surveillance is approved or disapproved, inventory notice should be served no less than thirty days and no more than ninety days after the emergency surveillance ends. This is because the reference to "authorization for electronic surveillance" in subdivision (a) includes an applicant's authorization for emergency surveillance pursuant to Standard 2-5.2, and is not limited to authorization by a court.

Standard 2-4.16. Disclosure; use

(a) A law enforcement officer should be permitted to disclose, receive or use the contents of a private communication intercepted by means of electronic surveillance conducted in a manner authorized by
these standards, or evidence derived therefrom, only to the extent it is in the proper performance of the officer’s official duties.

(b) Any person who is not a law enforcement officer should be permitted to disclose or use such a communication if the person obtains the contents of the communication lawfully and uses or discloses it for any lawful purpose.

Commentary to Standard 2-4.16

This Standard is derived from Standard 2-5.15 of the Second Edition, and includes a number of stylistic changes. Standard 2-5.15, for example, contained one provision permitting law enforcement officers to disclose lawfully intercepted communications, and evidence derived therefrom, “only to the extent that it is in the proper performance of their official duties,” and another provision that authorized them to disclose such evidence to other law enforcement officers only “to the extent that it is in the proper performance of their official duties to receive it.” Both of these provisions are collapsed into subdivision (a) of Standard 2-4.16. See 18 U.S.C. § 2517(1) (authorizing disclosure by one law enforcement officer to another “to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure”).

Standard 2-5.15 included a provision that “[a]ny person, including law enforcement officers, should be permitted to make such disclosures while giving testimony under oath or affirmation in a criminal proceeding or in a grand jury proceeding,” see also 18 U.S.C. § 2517(3). That provision was omitted from the present Standard because it is unnecessary, given that such testimony would be, within the meaning of subdivision (a) of present Standard 2-4.16 “in the proper performance of [a law enforcement] officer’s duties,” and other persons may give such testimony pursuant to subdivision (b) if they obtain the contents of the communication “lawfully” and the disclosure is “for any lawful purpose.” Note that while the omitted language limited its authorization for testimonial disclosure to criminal and grand jury proceedings, Standard 2-3.1(b)(i) recognizes the need to use lawfully intercepted communications not only in criminal proceedings, but also “in related civil actions,” for example, civil proceedings seeking forfeiture of the proceeds or instrumentalities of the crime which was the subject of the electronic surveillance.

Standard 2-5.15 also included a provision permitting the disclosure or use of intercepted communications, and evidence derived from such
communications, under circumstances not otherwise authorized by the Standard "only upon a showing of good cause before a judicial officer." This provision was also omitted from the present Standard on the theory that the Standard describes all the circumstances in which disclosure and use should be permitted, and that, in such circumstances, a showing of good cause to a judge is unnecessary. If, for example, intercepted communications were lawfully and publicly disclosed in a criminal trial, it would make no sense to require judicial approval of their use in a civil proceeding brought against the defendant by the victim of the crime for which the defendant was prosecuted, or in a book or article about the trial.\footnote{See also Bartnicki v. Vopper, 532 U.S. 514 (2001) (First Amendment protected media companies' broadcast of illegally intercepted telephone conversation where conversation was of public importance and companies had played no part in its illegal interception).}

Section 203(b) of the USA PATRIOT Act adds a new subdivision (6) to 18 U.S.C. 2517. This new subdivision permits "[a]ny investigative or law enforcement officer, or any attorney for the government" who lawfully obtains the contents of any wire, oral or electronic communication to disclose those contents "to any other Federal law enforcement, intelligence, protective, immigration, national defense, or national security official to the extent that such contents include "foreign intelligence," "counterintelligence," or "foreign intelligence information"\footnote{For purposes of this provision, the National Security Act defines "intelligence" as including "foreign intelligence and counterintelligence," and counterintelligence as "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons." 50 U.S.C. 401(a)(1) and (2). Also for purposes of this provision, 18 U.S.C. § 2510(19), as added by the USA PATRIOT Act, § 203A(b)(2), defines "foreign intelligence information" as "(A) information, whether or not concerning a United States person, that relates to the ability of the United States to protect against—(i) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; (ii) sabotage or international terrorism by a foreign power or an agent of a foreign power; or (iii) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or (B) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to—(i) the national defense of or the security of the United States; or (ii) the conduct of the foreign affairs of the United States."} when the purpose of the disclosure is "to assist the official receiving that information in the performance of his official duties." The official to whom this information is disclosed "may use that information only as necessary in the conduct of that person's official duties subject to any limitations on
the unauthorized disclosure of such information." Id.181 Because these provisions became law after the Task Force completed its work, the Standards do not explicitly consider whether disclosure for these purposes should be permitted. It seems apparent, however, that the disclosure of such information to an appropriate federal officer would be "in the proper performance of the [disclosing] officer's official duties" within the meaning of Standard 2-4.16. In commenting on this aspect of the USA PATRIOT Act before it was enacted, the American Bar Association's Task Force on Terrorism and the Law noted that "[i]t makes good sense to permit prosecutors to share with intelligence agencies information and to permit the reverse. To that extent, the Task Force understands the desire to change the language of FISA to reflect the realities of the need for cooperation among federal agencies."182

Standard 2-4.17. Reports

(a) Judges should make annual reports concerning electronic surveillance orders to an appropriate agency which should contain:

(i) the number of orders applied for;
(ii) the kinds of orders applied for;
(iii) the number of orders denied, the number granted as applied for, and the number granted as modified;
(iv) the periods of time over which electronic surveillance was conducted or records were made pursuant to each electronic surveillance order, including each extension of such an order;
(v) the offenses specified in the orders or the applications which were denied;
(vi) the identity of the persons authorizing the applications; and

181. Subdivision (c) of § 203 of the USA PATRIOT Act requires the Attorney General to establish procedures for disclosure of information pursuant to 18 U.S.C. § 2517(6) "that identifies a United States person." For this purpose, a "United States person" is defined as "a citizen of the United States, an alien lawfully admitted for permanent residence . . . , an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power . . . ." 18 U.S.C. § 1801(i).

(vii) the identity of the law enforcement agency of the applicant.

(b) Applicants should make annual reports concerning their applications to the agency specified in paragraph (a) which should contain:

(i) the information required in subdivisions (a)(i)–(vii);

(ii) a general description of the intercepting, separated by offense, including:

(A) the character and frequency of the incriminating communications intercepted;

(B) the character and frequency of the other communications intercepted;

(C) the number of persons whose communications were intercepted; and

(D) the character and amount of manpower and other resources used in the intercepting;

(iii) the number of arrests resulting from the intercepting;

(iv) the offenses for which the arrests were made;

(v) the number of trials in which intercepted communications, or evidence derived from intercepted communications, was used;

(vi) the number of motions to suppress made, granted, or denied based on the intercepting;

(vii) the number of convictions in cases in which intercepted communications, or evidence derived from intercepted communications, was used; and

(viii) the offenses for which the convictions were obtained.

(c) The agency specified in subdivisions (a) and (b) should make public a complete annual report based on the information required to be filed by subdivisions (a) and (b).

Commentary to Standard 2-4.17

This Standard is derived from Standard 2-5.16 of the Second Edition and contains only stylistic changes. Subdivision (a) requires reports from judges who issue electronic surveillance orders, and subdivision (b) requires reports from the applicants for such orders. Standard 2-5.16(b) of the Second Edition required that the latter reports come from "prosecuting officers." Subdivision (b) of the present Standard specifies that these reports should come from the applicants for electronic surveillance orders because it is one of the general principles of the Third Edition that the application for an electronic surveillance order be approved "by a politically accountable prosecutor with the authority to establish and maintain a uniform electronic surveillance policy.
within the affected jurisdiction," or their high ranking subordinates, and these reports are an important way in which applicants can be held accountable for their electronic surveillance policies. Obviously, the information required for some parts of these reports—e.g., the frequency of incriminating and non-incriminating communications—will necessarily be estimates.
PART V.
INTERCEPTION OF COMMUNICATIONS BY LAW ENFORCEMENT WITHOUT AN ELECTRONIC SURVEILLANCE ORDER

Standard 2-5.1. Intercepting communications with consent

(a) A law enforcement officer should be permitted to intercept the contents of a private communication with the consent of one of the parties to the communication without a court order, provided that the officer intercepts and uses the communication in the proper performance of the officer’s official duties.

Commentary to Standard 2-5.1(a)

This provision is derived from Standard 2-4.1 of the Second Edition, which provided that “[t]he surreptitious overhearing or recording of a wire or oral communication with the consent of, or by one of, the parties to the communication should be permitted without the necessity of a court order, provided such communication is not overheard or recorded for the purposes of committing a crime or other unlawful harm.” Note that, as modified, the present Standard takes no position concerning whether a person who is not a law enforcement officer should be permitted to intercept the contents of a private communication with the consent of a party to that communication. See the commentary to Standard 2-2.1(c)(iii). Because the present Standard relates only to the consensual interception of communications by law enforcement, it is appropriate that it permit such interception only “in the proper performance of the officer’s official duties,” rather than when it is not “for the purposes of committing a crime or other unlawful harm.”

(b) A law enforcement officer should be permitted to intercept the contents of the communications of an unauthorized user of an electronic communication service provider to or over that service without a court order when:

(i) the provider reasonably determines that the communications threaten to disrupt the provider’s service; and

(ii) the provider consents to the interception,
provided that the officer intercepts and uses the communications in the proper performance of the officer’s duties.

**Commentary to Standard 2-5.1(b)**

This provision has no counterpart in the First or Second Edition of the Standards, which permitted the warrantless interception of a communication by law enforcement only with the consent of one of the parties to the communication. It was added to permit a law enforcement agency to intercept, without a court order, the communications of a hacker who threatens to disrupt an electronic communication service provider, so long as the provider consents to the surveillance. Under Title III, when a communications service provider learns that an unauthorized user is engaging in activity that threatens to disrupt the provider’s service, the provider can monitor and intercept the communications of the unauthorized user transmitted over the provider’s service, 18 U.S.C. § 2511(2)(a)(i), and it can notify the law enforcement agency and disclose the intercepted communications to the agency after they are intercepted. 18 U.S.C. §2511(3)(b)(i). If the law enforcement agency decides to investigate the hacker, it can continue to accept the communications from the provider periodically—day by day, week by week, or after the end of the provider’s monitoring. Alternatively, the law enforcement agency can procure an electronic surveillance order authorizing it to intercept the communications itself, subject to all the limitations and regulations set forth in Title III. Even when such an order is obtained, however, the provider will likely continue to intercept the communications without a court order and without those limitations and regulations. Given that the user is an unauthorized one, and given that the provider will continue to monitor the user’s communications

---

183. These provisions are discussed in the commentary to Standard 2-8.1(b).

184. It sometimes happens that a service provider is first alerted to criminal use or interference with its facilities by law enforcement. If, as a result of receiving that information, the communications provider begins intercepting communications to detect and terminate the criminal conduct, and also discloses the communications to law enforcement for purposes of criminal prosecution, the question arises whether the service provider is intercepting the communications as an agent of law enforcement, thus requiring that the provisions of Title III for electronic surveillance by government be met. See, e.g., United States v. Perez, 118 F.3d 1, 6 (1st Cir. 1997) (pertinent factors in determining whether private party acted as agent of law enforcement include “the extent of the government’s role in instigating or participating in the search, its intent and the degree of control it exercises over the search and the private party, and the extent to which the private party aims primarily to help the government or to serve its own interests”).
and disclose them to the law enforcement agency, the user has no rea­sonable expectation of privacy, and the law enforcement agency should be authorized to intercept them with the provider’s consent.

Like the previous editions of the Standards, Title III has permitted the warrantless interception of a private communication by law enforce­ment only with the consent of one of the parties to the communication. As part of the new anti-terrorism law, however, the owner or operator of a ”protected computer” may authorize a person ”acting under color of law” to intercept the wire or electronic communications of ”a computer trespasser transmitted to, through or from the protected computer” if ”the person acting under color of law is lawfully engaged in an investiga­tion;” ”the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser’s communications will be relevant to the investigation;” and ”such interception does not acquire communications other than those transmitted to or from the computer trespasser.” 18 U.S.C. § 2511(2)(i), added by USA Patriot Act, § 217. This new federal provision, which was enacted after the Third Edition of the Standards was adopted, and which “sunset” on Decem­ber 31, 2005, appears considerably broader than Standard 2-5.1(b), since it does not require, as the Standard does, that the communications to be intercepted “threaten to disrupt the provider’s service,” and because the authority for warrantless surveillance may be triggered by the consent of the owner or operator of the protected computer, which may or may not be an electronic communication service provider.

(c) When a law enforcement officer intercepts the contents of a pri­vate communication with the consent of one of the parties to the com­munication pursuant to subdivision (a), or with the consent of an

185. For purposes of this definition, a “protected computer” is a computer: “(A) Exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government, or (B) which is used in interstate or foreign commerce or communication.” 18 U.S.C. §§1030(e)(2); 2510(20). A computer trespasser “(A) means a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer; and (B) does not include a person known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the pro­tected computer.” 18 U.S.C. 2510(21), added by USA PATRIOT Act, § 217.
Electronic Surveillance of Private Communications

2-5.1(c) (c)

Electronic communication service provider pursuant to subdivision (b), the officer should record it whenever reasonably possible and appropriate to do so, employing devices and techniques which will ensure that the record will be, insofar as practicable, complete and accurate. Administrative procedures should be followed in determining when it is not appropriate to make such a record, and when a record is made, procedures similar to those set forth in Standards 2-4.14, and 2-7.1 should be followed.

Commentary to Standard 2-5.1(c)

This provision is derived from Standard 2-4.1 of the Second Edition, which made it applicable only to communications intercepted with the consent of one of the parties. Standard 2-4.1 did not require that law enforcement officers record a consensually intercepted communication but only that, when they did, "they should employ devices and techniques that will ensure that the recording will be, insofar as practicable, complete, accurate and intelligible." The present Standard requires that a record be made of a consensually intercepted communication "whenever reasonably possible and appropriate to do so." Making a record will not always be possible either for technological or logistical reasons, or for a combination of both. For example, a face to face communication between a cooperating informant and the subject of an investigation may be impossible to record if it is too dangerous to install a recording device on the person of the informant and recording of the communication is not otherwise technologically possible. Even where it is possible to make a record of a communication, it may not be "appropriate" to do so. For example, making a recording of every communication of the tens of thousands of "buy and busts" that occur in major cities each year may be unduly burdensome and expensive. While, in a particular case, the failure to make such a recording may be an issue for the jury at trial, whether to avoid such issues by recording every undercover drug buy, no matter how small, is a question best addressed by police agencies and prosecutors and not by "black letter" Standards.

As is made clear by the reference to Standard 2-7.1, which requires that law enforcement agencies establish administrative regulations concerning the use of electronic surveillance techniques, the decision whether or not to record a consensually intercepted communication should be made pursuant to administrative guidelines. The reference to Standard 2-4.14, which concerns the authenticity of the records of the contents of communications intercepted non-consensually, establishes the
requirement that for consensual interceptions as well, the equipment and

techniques used should not only “enable the intercepting officers to make

a complete and accurate record of the intercepted communications,” but

should also “either protect an original record from editing or other alter-

ation, or disclose whether that record has been edited or altered.” See

the commentary to Standard 2-4.14(b). Standard 2-4.1 of the Second Edi-

tion also suggested that the administrative procedures for the recording

of consensual interceptions be “similar” to those set forth in Standard

2-5.13 of that edition, which required that recordings of non-consensual

communications be judicially sealed. As the Third Edition has rejected

judicial sealing for non-consensually intercepted communications (see

the commentary to Standard 2-4.14(b)), so it rejects it for consensually

intercepted communications.

Standard 2-4.1 of the Second Edition included a provision that

administrative procedures for recording consensually intercepted com-

munications “should be followed under the supervision of the principal

prosecuting attorney.” Because involvement of the principle prosecut-

ing attorney is required only for purposes of establishing and main-

taining accountability for a uniform electronic surveillance policy, and

because the consensual interception of communications does not con-

stitute electronic surveillance, this provision has been removed from the

Third Edition.

Standard 2-5.2. Intercepting communications in an

emergency situation

(a) When a law enforcement officer reasonably believes that an

emergency situation exists which involves substantial and imminent
danger to human life, the officer should be permitted to conduct elec-

cronic surveillance without a prior judicial order when:

(i) the law enforcement officer is authorized to intercept those

communications:

(A) in the case of a federal law enforcement officer, by the At-

orney General, the Deputy Attorney General or the Associate

Attorney General; or

(B) in the case of a state or local law enforcement officer, by the

principal prosecuting attorney of the state or local government,
or by a high ranking subordinate, when specifically permitted by
state law and when specially designated by the principal prose-
cuting attorney to authorize the interception of communications
in such a situation; and

(ii) the prosecuting official authorizing the interceptions pur-

suant to subdivision (i) first determines:

(A) that there are grounds consistent with these standards

upon which an order could be obtained authorizing an intercep-

tion; and

(B) because of the emergency, it is not practicable to make an

application for such an order before the communications are

intercepted.

(b) The requirements of making and protecting the integrity of a

record of the contents of the communications, set forth in Standard

2-4.14, shall be followed during any period of emergency surveil-

lance.

(c) Communications intercepted in conformance with Standard

2-5.2(a) may be disclosed and used in accordance with Standard 2-4.16

when:

(i) the prosecuting officer who authorized the interceptions, or

when that officer is absent or unavailable, another prosecuting offi-

cer who could have authorized the interceptions pursuant to Stan-

dard 2-5.2(a)(i), makes an application for an order approving the

interceptions to a judge with authority to issue an order authoriz-

ing the interceptions, had such an application been made;

(ii) the application sets forth the material facts upon which the

prosecuting officer relied in authorizing the interceptions;

(iii) the application is made within a reasonable period of time

but not more than forty-eight hours after the interception of com-

munications has begun;

(iv) the communications were otherwise intercepted in accor-

dance with these standards; and

(v) the judge to whom the application is made approves the

interceptions based upon a determination that the application
demonstrates that, at the time the prosecuting officer authorized the

interceptions:

(A) the law enforcement officer reasonably believed he was

confronted with the requisite emergency situation; and

(B) there were grounds consistent with these standards upon

which an order authorizing the electronic surveillance could

have been issued.
(vi) The judge to whom the application is made should be permitted to require the furnishing of additional facts under oath or information, which should be duly recorded.

d) Unless an application for approval is made and granted, the intercepted communications should be treated as impermissibly obtained pursuant to Standard 2-6.2(a) and an inventory filed as provided in Standard 2-4.15.

Commentary to Standard 2-5.2

Title III and the prior editions of the Standards have permitted electronic surveillance to be conducted without prior judicial authorization in an emergency situation. Although Title III also permits state law to authorize such emergency surveillance, not all states that have electronic surveillance statutes have authorized it. While some states make no special provision for emergencies, others require an application to and approval by a judge, but forgo the requirement that the application and/or approval be in writing.\(^{186}\) Although the possibility of requiring an oral application and order for emergency surveillance was considered, it was determined that such requirements were inappropriate where a showing could be made that, given an emergency of requisite gravity, making an application to a judge was not practicable. Thus, the Third Edition continues to permit warrantless emergency surveillance, but under more stringent requirements than did the previous editions.

Several issues arise in conducting emergency surveillance without a court order. The first is on whose authority it may be conducted. Under federal law, "an investigative or law enforcement officer" may engage in emergency electronic surveillance without a court order if the officer is "specially designated" to do so "by the Attorney General, the Deputy Attorney General, the Associate Attorney General or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State." 18 U.S.C. § 2518(7). Similarly, Standard 2-5.2 of the Second Edition permits a "specially designated" law enforcement

---

186. New York, for example, permits an application for a court order to be communicated to a judge "by telephone, radio or other means of electronic communication." New York Criminal Procedure Law § 7001.21(1). See also Carr, The Law of Electronic Surveillance (2000), at 3-150 (noting that "the eavesdropping statutes of some states respond to [the] problem of emergencies by requiring 'informal application' to a judge and his 'verbal approval' before commencing emergency surveillance") (footnote citing Delaware, New Jersey and Pennsylvania statutes omitted).
officer to conduct emergency electronic surveillance without a court order, and provides that the officer may be so designated by any of the officials authorized to apply for an order prospectively authorizing the interception of private communications, that is, "the Attorney General of the United States, the principle prosecuting attorney of a state or local government, or law enforcement officers acting under his or her direction." 187 Under both federal law and the previous Standards, the determination that emergency surveillance is necessary in a particular case must be made by the investigative or law enforcement officer, but not necessarily by the designating official. An official with designating authority may authorize a particular investigative or law enforcement officer to conduct emergency surveillance before any such emergency arises, leaving it to the officer alone to determine whether an emergency exists and whether electronic surveillance without a court order is justified. Neither Title III nor the previous Standards limited in any way which or how many investigative or law enforcement officers could be so designated.

Judge Carr has criticized Title III’s provisions as creating “dangers of excessive discretion in the officer,” and has recommended that “each instance in which the emergency surveillance is to be undertaken should be preceded by a special designation by the principal prosecuting attorney.” 188 Standard 2-5.2 of the Third Edition adopts that recommendation, permitting a federal law enforcement officer to conduct emergency electronic surveillance only when “authorized to intercept those communications” by “the Attorney General, the Deputy Attorney General or the Associate Attorney General,” and permitting a state law enforcement officer to do so only when authorized “by the principal prosecuting attorney of the state or local government, or by a high ranking subordinate.” Standard 2-5.2(a)(i). However, Standard 2-5.2 goes further, by requiring that before authorizing the emergency surveillance, the official must, himself or herself, first determine “that there are

187. Federal law is somewhat more restrictive than was Standard 2-5.2, to the extent that the list of federal officials who may designate a law enforcement officer to conduct emergency surveillance is shorter than the list of all of those who may authorize a federal application for a prospective order. Compare 18 U.S.C. § 2518(7) with 18 U.S.C. § 2516(1).

188. Carr, The Law of Electronic Surveillance (2000), at 3-147. Judge Carr adds that requiring prior designation particularly for the case in which it is used “ensures rudimentary control over the officer’s discretion, and increases the likelihood that necessary restrictions will be implemented and notice will be provided after the surveillance terminates.” Id.
grounds consistent with [the] standards upon which an order could be obtained authorizing an interception," and that "because of the emergency, it is not practicable to make an application for such an order before the communications are intercepted." Standard 2-5.2(a)(ii).189

The second question that arises in emergency electronic surveillance is for what kinds of emergencies it should be permitted. Title III limits its use to "an emergency situation . . . that involves—(i) immediate danger of death or serious physical injury to any person, (ii) conspiratorial activities threatening the national security interest, or (iii) conspiratorial activities characteristic of organized crime." Standard 2-5.2 of the Second Edition required "an emergency situation . . . involving substantial and imminent danger to human life."190 The Third Edition adheres to the requirement in the Second Edition, using identical language. Standard 2-5.2(a). Such situations rarely arise, and electronic surveillance should be conducted without a court order only in highly exceptional circumstances.191

The third question that arises is when, after the emergency surveillance is conducted, an application for an order approving the surveil-

---

189. Similarly, Standard 2-5.2 requires a determination, albeit by the law enforcement officer, that the emergency situation requires interception to occur "within such time that it is not practicable to make an application." Federal law, on the other hand, requires that the investigative or law enforcement officer determine that the emergency requires that communications be intercepted "before an order authorizing such interception can, with due diligence, be obtained." 18 U.S.C. 2518(7)(a). By using language different from that in Title III, the Standards do not intend to lessen the requisite showing. One court has held that when the authorities learned that electronic surveillance was necessary, but that the opportunity to intercept communications would last only two and a half hours, the requirement for conducting it without a court order had been satisfied. People v. Seehausen, 245 Ill. App. 3d 506, 615 N.E. 2d 376, 380 (1993).

190. Standard 5.2 of the First Edition, like Title III, required an emergency situation "with respect to conspiratorial activities threatening the national security interest or to conspiratorial activities characteristic of organized crime," but this language was deleted in the Second Edition. The commentary to Standard 2-5.2 of the Second Edition explained that national security was eliminated as a basis for emergency surveillance because other provisions of the Standards specifically authorizing electronic surveillance for national security "adequately cover that situation." The Third Edition of the Standards does not address national security electronic surveillance, either under "ordinary" circumstances, or in an emergency situation. See the introduction to this Edition.

191. See United States v. Capra, 501 F.2d 267 (1974) ("Congress had in mind by the use of the term 'emergency' an important event, limited in duration, which was likely to occur before a warrant could be obtained"), citing Senate Report No. 1097, 90th Cong., 2d Sess. 1968 Code Cong. & Admin. News 2112, 2193.
lance must be made. Federal law, as well as the previous editions of the Standards required that an application be made "within forty-eight hours after the interception has occurred, or begins to occur." 18 U.S.C. § 2518(7)(b). Standard 2-5.2(c)(iii) provides that the application must be made "within a reasonable period of time but not more than forty-eight hours after the interception of communications has begun." The purpose of the change is to encourage such applications to be made even earlier, since an earlier application may be "reasonabl[y]" possible. By encouraging earlier applications, however, the provision does not contemplate litigation in which a court is asked to second guess the applicant's ability to have made an application hours earlier than it was presented to the court.

The fourth question is who is permitted to make the application for an order approving the emergency electronic surveillance. Standard 2-5.2 of the Second Edition allows the intercepting officer to make the application, while 18 U.S.C. § 2518(7)(b), which requires that an application be made, does not specify who is authorized to make it. Consistent with the determination that an official with the authority for applying for an electronic surveillance be responsible for determining when emergency surveillance may be conducted without a court order, the present Standard requires that the application be made by "the prosecuting officer who authorized the interceptions, or when that officer is absent or unavailable, another prosecuting officer who could have authorized the interceptions pursuant to Standard 2-5.2(a)(i)."

Standard 2-5.2 of the Second Edition provided that "[t]he recording and return requirements of Standards 2-5.12 and 2-5.13 shall be followed during any period of emergency surveillance." Similarly, the present Standard mandates that "[t]he requirements of making and protecting the integrity of a record of the contents of the communication, set forth in Standard 2-4.14, shall be followed" during any such period. The return provision of Standard 2-5.13 of the Second Edition, including the requirement of judicial sealing of the recordings of the intercepted communications, has been omitted from the Third Edition. See the commentary to Standard 2-4.14(b). The requirement for a return can be satisfied for emergency electronic surveillance by including the requisite information in the application for the order of approval.

The present Standard makes explicit what was implicit in the earlier editions: that communications intercepted during emergency surveillance, as well as evidence derived therefrom, "may be disclosed and used in accordance with Standard 2-4.16" only if "the communications
were otherwise intercepted in accordance with [the] Standards. Standard 2-5.2(c)(iv).

Subdivision (d) of the present Standard provides that "[u]nless an application for approval is made and granted, the intercepted communications should be treated as impermissibly obtained pursuant to Standard 2-6.2(a) and an inventory [served] as provided in Standard 2-4.15." This subdivision is taken from a comparable provision in Standard 2-5.2(b) of the Second Edition and includes only stylistic changes.
PART VI.
SANCTIONS

Standard 2-6.1. Sanctions, in general

Except as otherwise permitted by these standards, electronic surveillance by any person should be expressly prohibited, and this prohibition should be enforced with appropriate criminal, civil, and evidentiary sanctions.

Commentary to Standard 2-6.1

This Standard is derived from a provision in Standard 2-1.1(b) of the Second Edition, and includes only stylistic changes that are not intended to affect its meaning.

Standard 2-6.2. Evidentiary sanctions; exceptions

(a) Except as otherwise expressly permitted under these standards, a private communication intercepted by a law enforcement officer by means of electronic surveillance, and any evidence derived therefrom, should not be received in evidence in any trial, hearing, or proceeding in or before any court, grand jury, department, officer, agency, regulatory body, or other authority.

Commentary to Standard 2-6.2(a)

This provision is derived from Standard 2-2.3 of the Second Edition of the Standards and contains only stylistic changes. See also 18 U.S.C. § 2515. It implements the general principle set forth in Standard 2-1.1(c)(v) that “[t]o further ensure the accountability of law enforcement officials and officers who participate in electronic surveillance, law enforcement agencies should . . . be subject to the exclusionary sanction in appropriate circumstances.” See the commentary to Standard 2-1.1(c)(v)(B).

(b) When a law enforcement officer intercepts a private communication by means of electronic surveillance conducted in a manner not expressly permitted by these standards, the communication, and any evidence derived therefrom, may nonetheless be received in evidence.
(i) in a prosecution for the unlawful interception of that communication; or

(ii) if the intercepted communication, or evidence derived therefrom, includes exculpatory information, and the defendant offers it in evidence, provided, however, that in response, the prosecution may offer evidence of, or derived from, that communication or another communication, if it would tend to rebut the evidence offered by the defendant pursuant to this subdivision.

Commentary to Standard 2-6.2(b)

This provision has no counterpart in the previous edition of the Standards, but expresses two commonsense notions. First, since the Standards recommend criminal sanctions for the unlawful interception of private communications (see Standard 2-6.3(b)(i)), they must also authorize the use of illegally intercepted communications in a prosecution for their illegal interception. Second, if a communication is illegally intercepted, the defendant—who, of course, is not required to seek its suppression [see Standard 2-6.2(f)]—may, in any case, use the communication in a criminal prosecution if the communication is exculpatory. Standard 2.6.2(b)(ii). However, as with other forms of evidence, suppression is a shield for a defendant, and not a sword for misleading a jury. Thus, if the defense does offer evidence of an illegally obtained communication, or evidence derived from that communication, the prosecution may offer evidence of or derived from that communication, or another communication, "if it would tend to rebut the evidence offered by the defendant pursuant to this subdivision."192

(c) When a prosecuting attorney intends to offer evidence of the contents of communications obtained by a law enforcement officer by

192. See United States v. Havens, 446 U.S. 620 (1980) (statements a defendant makes in response to proper cross examination reasonably suggested by defendant's direct examination may be impeached by admission of illegally obtained evidence not admissible as part of prosecution's direct case). Judge Carr predicts that in light of Havens, § 2515 will ultimately be construed by the Supreme Court as permitting impeachment use of suppressed recordings," 2 Carr, The Law of Electronic Surveillance (2000), at 7-137, and he notes that a number of lower courts have already held that where electronic surveillance evidence "has been otherwise suppressed, it is admissible to impeach a witness or the defendant." Id. at 7-138 (footnotes with case citations omitted).
means of electronic surveillance, or evidence derived therefrom, the prosecuting attorney should give notice of that intention within a reasonable period before trial, and should disclose to the defendant at that time:

(i) the order or orders pursuant to which the electronic surveillance was conducted;

(ii) the applications for those orders;

(iii) the progress reports submitted to the court pursuant to those orders;

(iv) copies of the records of the communications the prosecuting attorney intends to offer in evidence; and

(v) such other material as may be required by the judge before whom the suppression motion referred to in subdivision (f) is made for purposes of the motion.

Commentary to Standard 2-6.2(c)

This provision replaces Standard 2-2.3 of the Second Edition of the Standards, which provided that "[t]he standards set forth in chapter 11 of these standards [relating to Discovery and Procedure Before Trial] should apply to disclosure by the prosecution in a criminal case of information relating to use of electronic surveillance techniques and to evidence derived therefrom." The present Standard more specifically indicates which documents the defendant will need to prepare a motion to suppress. For purposes of this provision, "a reasonable period of time" is that time necessary to permit motions to be made and decided in a timely fashion concerning the admissibility of the evidence obtained by and derived from the electronic surveillance. Compare 18 U.S.C. 2518(9), which provides that the contents of any intercepted communication may not be offered in evidence "unless each party, not less than ten days before the trial, hearing or proceeding, has been furnished with a copy of the court order, and accompanying application, under which the interception was authorized or approved." Ten days seems exceedingly short for the intended purpose.

(d) For the purpose of protecting the privacy of any person who is not a subject of the prosecution, the court may, upon the application of the prosecuting attorney or the defendant, or sua sponte, issue a
protective order prohibiting or regulating the disclosure to others of the contents of these materials.

Commentary to Standard 2-6.2(d)

This provision is new and reflects the fact that discovery of electronic surveillance materials can adversely impact the privacy interests of persons who are not parties to the criminal action in which the discovery is made. Persons whose privacy rights may thus be harmed include those who were parties to or mentioned in intercepted communications. Harm is particularly inappropriate when, in the process of minimization, communications were intercepted which were not pertinent to the crimes that were the authorized subject of the electronic surveillance. Litigation over the admissibility of electronic surveillance evidence, and the introduction of such evidence in hearings and trials, may inevitably result in the revelation of matters embarrassing to third parties. Nonetheless, consistent with the needs of the litigation and with the First Amendment, a judge should be able to issue orders to prohibit or regulate disclosure in order to protect the legitimate privacy interests of third parties.

(e) When the prosecutor gives notice pursuant to subdivision (c) of this standard of the intent to offer evidence obtained by means of electronic surveillance, if communications obtained by the electronic surveillance were minimized pursuant to Standard 2-4.9:

(i) the court should order that the communications that the minimizing officer determined were not otherwise subject to interception be disclosed to the defendant;

(ii) if the defendant intends to offer in evidence the contents of any of those communications in any proceeding, the defendant should give notice of that intention to the prosecutor within a reasonable period of time before the proceeding;

(iii) if the defendant gives such notice, the court should order, upon request of the prosecutor, that the communications disclosed to the defendant pursuant to subdivision (i) be disclosed to the prosecutor; and

(iv) when communications are disclosed to the defendant pursuant to subdivision (i), or to the prosecutor pursuant to subdivision (iii), the court should issue a protective order prohibiting or regulating the disclosure of those communications to others.
Commentary to Standard 2-6.2(e)

One of the more controversial subjects to be considered by the Third Edition of the Standards was whether and when a defendant should receive disclosure of communications, or portions of communications, that were determined in after-the-fact minimization conducted pursuant to Standard 2-4.9 not to be relevant to the crime that was the authorized subject of the electronic surveillance. See the commentary to Standard 2-4.9(a). Resolution of this issue required balancing the rights of the defendant against the privacy rights of those, other than the defendant, who were parties to those communications. A variety of approaches were considered, and a variety of decisions made, as the Standards moved along toward their ultimate approval. One possible approach was to recognize that, in effect, those communications would not have been intercepted had contemporaneous minimization been possible, and to respect the privacy of those communications by treating them as if they had never been intercepted—that is, by forbidding their disclosure. That approach was rejected from the outset for two reasons: because some of those communications could contain information that tended to exculpate the defendant, and because some of the communications, whether or not exculpatory, would be the defendant’s own, and for those communications, no privacy interest was served by forbidding their disclosure to the defendant.

In drafting the Third Edition of the Standards, the Task Force on Technology and Law Enforcement resolved this question initially by requiring disclosure to the defendant and the prosecuting attorney of any communications determined after the fact not to be subject to interception if the defendant could establish probable cause to believe that those communications include exculpatory information. The Task Force would also have allowed disclosure to the defendant of all such communications to which he or she was a party, and to the prosecuting attorney of those of the defendant’s communications that the defendant intended to use at trial. Under the Task Force provisions, the court could also order disclosure of any other of the minimized communications “for good cause shown.”

193. The Task Force provided, however, that if any such exculpatory communications were disclosed to the defendant, the judge could disclose to the prosecuting attorney and the defendant any other minimized communications tending to rebut the communications disclosed to the defendant.
Although these provisions were accepted by the Criminal Justice Standards Committee, the Criminal Justice Council rejected them, because of the difficulty a defendant would inevitably have in demonstrating probable cause that communications not disclosed to the defendant contained exculpatory material.194 The Council decided instead that the defendant should be entitled to all the intercepted communications that the minimizing officer determined were not otherwise subject to interception, Standard 2-6.2(e)(i), and that the prosecuting attorney should be entitled to them as well, if the defendant gave notice of his intent to offer any of them in evidence in any proceeding, Standard 2-6.2(e)(iii). Recognizing that this approach would result in every case in the disclosure of all of the intercepted communications of persons who were not parties to the case, the Council added a provision requiring the court to "issue a protective order prohibiting or regulating the disclosure of those communications to others." Standard 2-6.2(e)(iv). The House of Delegates approved these provisions as they were revised by the Council.

When minimization is accomplished after the fact, some of the communications minimized after their interception might be privileged. Standard 2-6.2(e) is not, however, intended to permit the wholesale disclosure of privileged communications. When contemporaneous minimization is possible, privileged communications are simply not "subject to interception." See Standard 2-2.1(e)(ii). When contemporaneous minimization is not possible, any and all privileged communications will necessarily be intercepted, but they remain privileged despite their interception. Indeed, Standard 2-4.12(b) specifically provides that "[n]o otherwise privileged communication intercepted in accordance with or in violation of these standards should lose its privileged character."

It is, of course, perfectly appropriate for the defendant to receive disclosure of his or her own privileged communications, and equally appropriate for the court to issue, on the defendant’s application, a protective order preventing their disclosure to the prosecution.195 Although a defendant who serves notice of the intent to use one or more of the minimized communications thereby triggers the prosecution’s right to disclosure, the service of that notice should not constitute a waiver of

194. Indeed, the Council considered, and rejected for the same reason, requiring a lesser threshold, "a reasonable possibility" to believe that the minimized communications included exculpatory information.

195. In an appropriate case, a defendant should also be permitted to seek a protective order to prevent the disclosure of his or her privileged communications to a co-defendant.
any privilege the defendant holds with respect to any of the intercepted communications.\textsuperscript{196} No less significantly, unminimized communications subject to disclosure pursuant to Standard 2-6.2(e) may include the privileged communications of someone other than the defendant, and when it is known that such communications exist, they should be disclosed neither to the defendant nor the prosecution. Thus, before any minimized communications are disclosed—in the first instance to the defendant, or, thereafter, to the prosecution—if there is reason to believe that they include privileged communications, either side may (and should) request the court to have the unminimized communications reviewed—perhaps by a special master—so that the privileged communications of any third party may be excluded from the disclosure. After minimized communications are disclosed to and reviewed by the defendant or the prosecution, if either determines that the material includes the privileged communications of a third party, a protective order should be sought preventing their further disclosure.

\textit{(f) Any party aggrieved by the interception, use, or disclosure of private communications by law enforcement, or of evidence derived therefrom, otherwise than as expressly permitted under these standards, should be permitted to move to suppress those communications or that evidence. The motion should be made prior to the trial, hearing, or other proceeding unless there was no opportunity to make the motion or the party was unaware of the grounds on which the motion could be made. Where such a motion is made and granted, prior to the attaching of jeopardy, during the course of a criminal prosecution, the prosecuting attorney, where necessary, should be afforded a right of appeal provided that the appeal is not taken for the purpose of delay and is diligently prosecuted.}

\textit{Commentary to Standard 2-6.2(f)}

This provision is derived from Standard 2-2.3(c) of the Second Edition, and contains only stylistic changes.

\textsuperscript{196} If, of course, a defendant intends to offer a privileged communication in evidence, by doing so the defendant waives the privilege with respect to that communication.
(g) Such evidence should be suppressed if:

(i) the communications were obtained in violation of the Constitution of the United States, or, in the case of an order issued by a state or local judge, of the state constitution;

(ii) the communications were obtained pursuant to an order issued by a judge other than as permitted by Standard 2-4.1, or upon an application made by an applicant other than as permitted by Standard 2-4.2, or upon an application failing to make one of the showings required by Standard 2-4.3; or

(iii) the evidence is obtained in violation of a statutory provision designed to enforce one of the general principles set forth in these standards governing electronic surveillance, unless the violation was committed in reasonable reliance upon an electronic surveillance order.

Commentary to Standard 2-6.2(g)

Independent of any statutory provision, intercepted communications must be suppressed if they were obtained in violation of the Fourth Amendment. Beyond that, federal statutory law provides for suppression of intercepted wire and oral communications, and of evidence derived from such communications, in 18 U.S.C. § 2515, “if the disclosure of that information would be in violation of [Title III].” In turn, 18 U.S.C. § 2518(10)(a) sets forth the grounds for the statutory suppression remedy: that “the communication was unlawfully intercepted;” that “the order of approval under which it was intercepted is insufficient on its face;” or that “the interception was not made in conformity with the order of authorization or approval.” These statutory suppression provisions have no application to intercepted electronic communications, that is, those that do not include the human voice, and thus such communications are subject to suppression under federal law only on constitutional grounds.197 Among those provisions of Title III which are not constitutional in origin (and thus for violation of which suppression of electronic communications may not be an available remedy) is the requirement that electronic surveillance be

---

197. The legislative history to the Electronic Communications Privacy Act offers no rationale for excepting electronic communications from statutory suppression, indicating only that the exception was made “as the result of discussions with the Justice Department.” Senate Report No. 99-541, 99th Cong. 2d Sess., 1986 U.S. Code Cong. & Admin. News 3555, 3577.
employed only when other means of investigation cannot achieve the objectives of the surveillance. 198

Interpreting these statutory provisions, the Supreme Court has held that suppression should result only when the violated provision "was intended to play a central role in the statutory scheme,"199 and only for noncompliance with "any of the statutory requirements that directly and substantially implement the Congressional intention to limit the use of intercept procedures to those situations clearly calling for the employment of this extraordinary device."200 In applying these criteria, the Supreme Court has determined that "the provision for pre-application approval [by a senior official in the Department of Justice] was intended to play a central role in the statutory scheme,"201 but identifying in the application for an electronic surveillance order those likely to be heard in incriminating communications and serving inventory notice on the subjects of the surveillance do not.202 The Tenth Circuit has also held that the necessity requirement also "directly and substantially implements the congressional intention to limit the use of intercept procedures to those

201. United States v. Giordano, 416 U.S. 505, 527 (1974). On the other hand, identifying the authorizing official in the application did not play such a central role, so that misidentifying the official did not require suppression if the official who, in fact, authorized the application could lawfully do so. United States v. Chavez, 416 U.S. 562 (1974). In Chavez, the Court conceded that identification of the authorizing official serves several purposes: it facilitates the ability of the court issuing the warrant to determine that an application has been approved by an appropriate official; serves to "fix responsibility" for the decision to make the application; and aids the issuing court, the authorizing official, and the Administrative Office of the United States Courts to fulfill their various reporting requirements. 416 U.S. at 575–77. Nonetheless, the Court found that adherence to the requirement that the applicant be identified in the application "does not establish a substantive role to be placed in the regulatory system." 416 U.S. at 578.
202. United States v. Donovan, 429 U.S. 413, 436 (1977). In United States v. Ojeda Rios, 495 U.S. 257, 260 (1990), the Supreme Court noted that 18 U.S.C. 2518(8)(a)(2), which requires that tapes be sealed "immediately" after the conclusion of the authorized period of eavesdropping, includes its own "explicit suppression remedy" by providing that "[t]he presence of the seal provided for by this subsection, or a satisfactory explanation for the absence thereof, shall be a prerequisite for the use or disclosure of the contents of any wire, oral, or electronic communication or evidence derived therefrom. . . ." Thus, the Court held that the general suppression remedy set forth in 18 U.S.C. § 2518(10) has no application to a sealing violation. Since that general suppression remedy does not apply, neither does its "central role" test.
situations clearly calling for their employment, and that violation of this requirement thus also requires suppression. While some state courts have adhered to the "central role" test, others have ordered the suppression of wire and oral communications for additional statutory violations, and some for violation of virtually any statutory provision.

The Second Edition, like the First, contained no provision explaining what violation of the Standards should result in suppression. The commentary to Standard 2-2.3 of the Second Edition did, however, observe that "[s]uppression does not occur for every failure to follow the procedures established by these standards," and suggested that, as for Title III,

203. United States v. Mondragon, 52 F.3d 291, 294 (10th Cir. 1995). See, however, United States v. Vento, 533 N.2d 838, 861–2) (3d Cir. 1976) (failure to include minimization provision in eavesdropping warrant as required by Title III did not require suppression, where despite the absence of the minimization provision, the agents were instructed to carry out minimization procedures, they in fact did so, and progress reports were submitted to the court which permitted it to closely supervise the execution of the warrant); United States v. Cirillo, 499 F.2d 872 (2d Cir. 1974) (same). For a collection of lower court decisions finding that various provisions of Title III are not "central" to the statutory scheme of Title III, see 2 Carr, The Law of Electronic Surveillance (2000), at 6-72–6-73.

204. For a review of the variation in state law suppression rules, see 2 Carr, The Law of Electronic Surveillance (2000), at 6-68.1–6-68.2. New York is a prime example of a state that requires suppression for violations not central to the statutory scheme. See, e.g., People v. Gallina, 66 N.Y.2d 52 (1985) (failure to make permanent deactivation "as soon as practicable" after expiration of warrant requires suppression; application for extension must be made before expiration of warrant, and making of application for extension after expiration requires suppression); People v. Winograd, 68 N.Y.2d 383 (1986) (suppression required because of unexplained failure to contact issuing justice over weekend and failure to seal before another justice when issuing justice unavailable on religious holiday). Judge Carr cites Maryland, Oregon and Rhode Island as other states that "have adopted the position that strict compliance, rather than simply substantial compliance with statutory requirements is expected, and will be required." Carr, supra, at 6-71–6-72 (footnote with citations to state court opinions omitted).

205. As originally drafted in 1968 by the Advisory Committee on the Police Function, Standard 2.3 of the First Edition explicitly provided that "[a]n error not affecting substantial rights in an application, authorization, or overhearing or recording of the otherwise authorized overhearing or recording of wire or oral communications should not be grounds for the suppression of such communications or evidence derived therefrom," and that "[e]xcusable error in the process of securing authorization for the overhearing and recording of such communications should be subject to cure by judicial ratification." This language, (which Judge Carr notes was effectively adopted by the Supreme Court in Giordano and Chavez, see 2 Carr, The Law of Electronic Surveillance (2000), at 6-71) was dropped from the Standard by the Special Committee on Standards for the Administration of Criminal Justice, which, on the recommendation of the Criminal Law Council, and by a vote of 7-5, took the position that "these matters are best handled on a case-by-case basis and need not be stated in the text of the standards themselves." See the commentary to Standard 2.3 of the First Edition.
it should be limited to the violation of provisions that play a "central role" in the Standards. The commentary emphasized, however, that "[t]he basic procedures for court-ordered electronic surveillance established by these standards are not mere technicalities; they are essential protections against excessive intrusion into conversational privacy." (Emphasis added.) Accepting the notion that violations of "core" or "basic" provisions should require suppression, and that lesser violations should not, Standard 2-6.2(g) identifies, more precisely than does Title III, which provisions are those "core" or "basic" ones. Moreover, the present Standard, unlike Title III, does not differentiate aural from non-aural communications, and provides the same grounds for suppressing communications that do not include the human voice as for those communications that do.

Standard 2-6.2(g) divides the grounds for suppression into three categories. First, and most obviously, electronic surveillance evidence should (and must) be suppressed "if the communications were obtained in violation of the Constitution of the United States, or, in the case of an order issued by a state or local judge, of the state constitution. Second, electronic surveillance evidence should be suppressed if "the communications were obtained pursuant to an order issued by a judge other than as permitted by Standard 2-4.1," that is, a judge who is not "of the highest court of general trial jurisdiction, or a court authorized to hear appeals from that court," or if they were obtained "upon an application by an applicant other than as permitted by Standard 2.4.2," that is, by an applicant not authorized by Standard 2-4.1(b) to make an application for an electronic surveillance order; or if they were obtained "upon an application failing to make one of the showings required by Standard 2-4.3," that is, one failing to establish probable cause to believe a person is committing, has committed, or is about to commit a particular designated offense, probable cause that evidence of the offense may be obtained by the electronic surveillance sought, and that the objectives of the electronic surveillance cannot be achieved by other means of investigation.206

The third and final category provides for suppression of electronic surveillance evidence if it is obtained "in violation of a statutory provision designed to enforce one of the general principles set forth in these Standards governing electronic surveillance." In other words, the violation must be such that admission of the evidence would contravene one

---

206. Failure to make either of the two probable cause showings, would, of course, also constitute a Fourth Amendment violation, thus rendering the intercepted communications subject to suppression under the first category, because they were "obtained in violation of the Constitution of the United States."
of those principles set forth in Standard 2-3.1 concerning the need to protect private communications, the need to allow regulated electronic surveillance by law enforcement, or the application for and execution of an electronic surveillance order. For this final of the three suppression categories, Standard 2-6.2(g)(iii) adopts a "good faith" exception. Pursuant to that exception, electronic surveillance evidence obtained in violation of a statutory provision designed to enforce the general principles should nonetheless be received in evidence, if "the violation was committed in reasonable reliance upon an electronic surveillance order." This "good faith" exception is adopted from the opinions of the Supreme Court in United States v. Leon and Massachusetts v. Sheppard,207 and adopts the logic of those opinions that the purpose of suppression—deterrence of unlawful conduct—will not be advanced by the suppression of evidence obtained by law enforcement officers who, in doing so, are reasonably relying on the order of a court.208 By a statutory amendment in 1986, Congress adopted the good faith exception for electronic surveillance when the violation is of "a constitutional magnitude."209

207. In United States v. Leon, 468 U.S. 897 (1984), the Court held that evidence obtained in objectively reasonable reliance on a search warrant later invalidated for failure to establish probable cause should not be suppressed. In Massachusetts v. Sheppard, 468 U.S. 981 (1984), the Court held that evidence obtained in the execution of a search warrant that was defective in form should not be suppressed if the officers executing the warrant reasonably believed that the warrant was not defective.

208. In United States v. Ojeda Rios, 495 U.S. 257 (1990), the Supreme Court accepted a "good faith" exception to suppression of electronic surveillance evidence in a different context: a delay of more than eighty-two days in the sealing of recordings of intercepted communications. On appeal, the government alleged that the delay was based upon the assumption that an order obtained after the expiration of the order pursuant to which the tapes were intercepted was an extension of that earlier order, and thus postponed the sealing requirement until expiration of the authorization in the new order. The Court held that the assumption, while erroneous, was objectively reasonable, and would provide a "satisfactory explanation" for the delay within the meaning of 18 U.S.C. § 2518(8)(a). Thus, in Ojeda Rios, the error was occasioned by objective reliance on a mistaken interpretation of a statutory provision, rather than by objective reliance on a defective court order.

209. 2 Carr, The Law of Electronic Surveillance (2000), at 6-88. The amendment added a new subdivision (c) to 18 U.S.C. § 2510(10), which provides that "[t]he remedies and sanctions described in this chapter with respect to the interception of electronic communications are the only judicial remedies and sanctions for nonconstitutional violations of this chapter involving such communications." The legislative history of that amendment states that "[i]n the event that there is a violation of law of constitutional magnitude the court involved in a subsequent criminal trial will apply the existing constitutional law with respect to the exclusionary rule," citing, inter alia, Leon and Sheppard. See Carr, id., 6-88.1. For a collection of electronic surveillance cases applying the good faith exception, see, id., at 6-88.1–6-89.
(h) When a person who is not a law enforcement officer intercepts the contents of a private communication in a manner not authorized pursuant to these standards or prohibited by law, a law enforcement officer should not be permitted to receive and use that communication unless:

(i) the person who intercepts the communication does not do so as an agent of a law enforcement officer;

(ii) the officer receives and uses the communication in the proper performance of the officer’s duties; and

(iii) the communication is used with respect to a crime in which physical injury to a person or serious physical damage to property is caused or threatened.

In exercising discretion to use a communication so intercepted in a criminal prosecution, the prosecuting attorney should consider the manner in which the communication was obtained and the effect of its use on privacy.

Commentary to Standard 2-6.2(h)

Generally, when evidence is illegally obtained without the involvement of law enforcement, the “clean hands” doctrine permits its use, on the theory that the Fourth Amendment “is wholly inapplicable ‘to a search and seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official.’”210 However, 18 U.S.C. 2515 prohibits the testimonial use of wire and oral communications that are unlawfully intercepted by any person, including someone who is not a law enforcement officer or acting as an agent for one.211 Based on this provision, courts have generally held that the fact that “an unlawful recording has been made without police or prosecutorial involvement, and receipt of the recording by law enforcement officers involved no culpability on their part” does not justify admitting the recording in evidence.212 Standard 2-2.3 of the Second Edition similarly

211. 18 U.S.C. § 2515 prohibits the testimonial use of wire and oral communications “if the disclosure of that information would be in violation of [Title III].” Because § 2515 does not apply to unlawfully intercepted electronic communications, it does not prevent application of the “clean hands” doctrine in such cases.
prohibits the evidentiary use of illegally intercepted private communications “[e]xcept as otherwise expressly permitted under these standards,” without distinguishing between the interception of communications by those who are in law enforcement and by those who are not.

The Third Edition of the Standards, like Title III, is designed to protect private communications from unlawful interception by private parties as well as by law enforcement, and thus continues to ban application of the “clean hands” doctrine to the unlawful interception of most communications by someone not affiliated with or acting on behalf of law enforcement. It concludes, however, that the interest in privacy is outweighed when a private party unlawfully intercepts a communication relating to a crime in which “physical injury to a person or serious physical damage to property is caused or threatened,” and that the “clean hands” doctrine should be applicable in the prosecution of such a crime.

By permitting the testimonial use of illegally intercepted communications relating to crimes of physical injury or serious physical damage to property, Standard 2-6.2(h) does not intend to encourage private illegal electronic surveillance. To the contrary, the Standards recommend that a prosecutor who is considering the use of a private communication so obtained to first “consider the manner in which the communication was obtained and the effect of its use on privacy.” Moreover, private persons who unlawfully intercept communications should be prosecuted for that conduct vigorously, regardless of whether the communications they intercept are or may be used in court pursuant to this provision. Such unlawful surveillance remains subject to civil sanctions as well.

**Standard 2-6.3. Criminal sanctions**

(a) The possession, sale, distribution, advertisement, and manufacture of devices primarily useful for the surreptitious interception of private communications should be regulated in order to prevent the use of such devices in a manner not authorized by these standards.

(b) The following conduct should be made criminal:

(i) the intentional interception of private communications by means of electronic surveillance conducted in a manner not authorized by these standards;

1404 (6th Cir. 1995) (holding that “the government is entitled to a ‘clean hands’ exception to 18 U.S.C. § 2515”).
(ii) the intentional use or disclosure of private communications intercepted by means of electronic surveillance, or evidence derived therefrom, when the electronic surveillance is conducted in a manner not authorized by these standards, or when the communications are used or disclosed in such an unauthorized manner;

(iii) the possession, sale, distribution, advertisement, or manufacture of a device primarily useful for the surreptitious interception of private communications in violation of a regulation adopted pursuant to Standard 2-6.3(a); and

(iv) the intentional promotion, whether by advertising or otherwise, of any device for use in intercepting such communications in a manner not authorized by these standards.

(c) Any device possessed, used, sold, distributed, or manufactured in violation of these prohibitions or regulations should be subject to confiscation.

Commentary to Standard 2-6.3

This Standard is derived from Standard 2-2.1 of the Second Edition. While it includes structural and wording changes, they are stylistic only.

Standard 2-6.4. Civil sanctions

(a) Except as otherwise expressly permitted by these standards, the use of electronic surveillance, or the use or disclosure of a communication intercepted by means of electronic surveillance, or evidence derived therefrom, should give rise to a civil cause of action against any person or governmental agency who so conducts the electronic surveillance, or knowing or having reason to know that such communication or evidence was obtained by electronic surveillance, who so discloses or uses such communication or evidence derived therefrom, or procures or authorizes another to do so.

(b) Good faith reliance on a court order or other legislative authorization should constitute a complete defense to civil recovery.

Commentary to Standard 2-6.4

This Standard is derived from Standard 2-2.2 of the Second Edition, and includes only stylistic changes.
PART VII:
ADMINISTRATIVE REGULATIONS

Standard 2-7.1. Administrative regulations

(a) Law enforcement agencies should adopt administrative regulations, including standards, procedures, and sanctions, dealing with the various aspects of the use of electronic surveillance techniques. The regulations, among other things, should:

(i) limit the number of officers in the agency authorized to employ the techniques;
  (ii) specify the circumstances under which the techniques may be used, giving preference to those which invade privacy least;
  (iii) set out the manner in which the techniques must be used to assure authenticity;
  (iv) require that officers who execute electronic surveillance orders first be trained in the law and techniques of electronic surveillance;
  (v) require the close supervision of officers authorized to employ the techniques;
  (vi) permit an officer to execute an order authorizing electronic surveillance only after the officer has read the order and the application, and has been instructed by the prosecuting attorney concerning the crime for which electronic surveillance has been authorized, the objectives of the electronic surveillance, the parties whose communications may be intercepted, the types of communications which may be intercepted, and the obligation to minimize the interception of communications which are not otherwise subject to interception;
  (vii) circumscribe the acquisition of, custody of, and access to electronic equipment by agents; and
  (viii) restrict the transcription of, custody of, and access to overheard or recorded communications by agents.

(b) Materials on the regulations should be incorporated into general and special training programs of the agency.

Commentary to Standard 2-7.1

This Standard is derived from Standard 2-5.17 of the Second Edition, and includes changes which are primarily stylistic. Subdivisions (iv) and (vi) of subsection (a) are, however, new. Subdivision (iv) requires
training in the law and techniques of electronic surveillance. While such training may come from the applicant for a particular electronic surveillance order, it is also advisable that agencies whose officers routinely execute electronic surveillance orders train those officers as well. See the commentary to Standard 2-3.1(c)(ii)(B). If the agency frequently works with a particular applicant or a particular supervising prosecutor, consultation with that officer will assure that the training is consistent with the procedures the officer employs. The prosecuting attorney who supervises the execution of an electronic surveillance order should, of course, permit the order to be executed only by officers who have "read the order and the application, and ha[ve] been instructed by the prosecuting attorney concerning the crime for which electronic surveillance has been authorized, the objectives of the electronic surveillance, the parties whose communications may be intercepted, the types of communications which may be intercepted, and the obligation to minimize the interception of communications which are not otherwise subject to interception." Nonetheless, the administrative regulations of the law enforcement agency that assigns officers to execute the order should include the same requirement, since those regulations will be directly binding on those officers.
PART VIII.
PRIVATE COMMUNICATIONS ACQUIRED BY AND RECEIVED FROM ELECTRONIC COMMUNICATION SERVICE PROVIDERS

Standard 2-8.1. Communications acquired by an electronic communication service provider

(a) An electronic communication service provider not offering its services to the public, and the principals, employees and agents of such a provider, should be permitted to acquire, use and disclose the contents of the private communications transmitted over or stored with its service for any lawful purpose.

Commentary to Standard 2-8.1(a)

This subdivision and subdivision (b) concern when a communication service provider may acquire, use and disclosure private communications it transmits or stores. This subdivision applies to providers who do not offer their services to the public, while subdivision (b) applies to public providers. Although the previous editions of the Standards included no comparable provisions, and were silent concerning the acquisition, use and disclosure of communications by private and public providers, federal law regulates such conduct by both. Under 18 U.S.C. 2511(2)(a)(i), "an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication [may] intercept, disclose or use that communication in the normal
2-8.1(a) Electronic Surveillance of Private Communications

course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights of property of the provider of that service.\(^{215}\) While 18 U.S.C. § 2702 regulates the disclosure of communications stored with a public electronic communication service provider, it places no constraints on the disclosure of communications stored with a private provider. Until recently, a "wire communication" was defined to include "any electronic storage of such communication," 18 U.S.C. § 2510(1), and thus a wire communications service provider—public or private—could disclose a stored wire communication only under those circumstances in which the provider could disclose an intercepted one. See 18 U.S.C. § 2511. Now, however, § 209(2) of the USA PATRIOT Act has amended the definition of a "wire communication" in 18 U.S.C. 2510(1), excluding a stored wire communication from the definition of that term.\(^{216}\) As a result, stored wire communications are subject to the same disclosure rules as stored electronic communications, and private service providers are unconstrained in their disclosure of all stored communications—whether or not the communications include the human voice.

While federal law thus gives both public and private communication service providers broad authority to intercept, use and disclose wire and electronic communications transmitted over and stored with their services, Standard 2-8.1 gives private providers even broader authority, by permitting them to do so "for any lawful purpose."\(^{217}\) The breadth of the authority the Standard provides gives appropriate recognition to both a private provider's right to control the use of services it provides

\(^{215}\) For this and other purposes, 18 U.S.C. § 2510(15) defines "electronic communication service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. 2511 (2)(a)(i) places one limitation on the authority of the provider of such a service to intercept, disclose and use communications transmitted over the service, which is applicable only to "a provider of wire communication service to the public," and which prohibits a public provider from utilizing "service observing or random monitoring except for mechanical or service quality checks." Note that this limitation is not applicable to public providers of electronic (that is, non-aural) communication services.

\(^{216}\) Note, however, that § 209 of the USA PATRIOT Act "sunsets" on December 31, 2005. USA PATRIOT Act, § 224.

\(^{217}\) Under the Standards, a private communication is an "electronic" one even if it includes the human voice, see Standard 2-2.1(1). Thus, because the regulations in Standard 2-8.1, and throughout Part VIII of the Standards, are applicable to any "private communication," they are applicable alike to both "wire" and "electronic" communications, as federal law defines those terms.
Electronic Surveillance of Private Communications 2-8.1(b)(i)

to its employees for its own convenience and for its own purposes, and to a private provider’s power, either by contract or consent, to require employees who use its service to surrender whatever expectation of privacy they might otherwise have in the communications transmitted over or stored with it. Private providers, however, should not use this authority arbitrarily, and instead should develop reasonable protocols for accessing such communications. Such protocols, if disclosed, will give fair notice to employees of the type and degree of monitoring to expect, and can be useful in demonstrating, should the need arise, that an employer exercised “due diligence” in preventing its employees from using its service in unauthorized ways that proved harmful to others.

(b) A public electronic communication service provider, and its principals, employees and agents, should be permitted to acquire, use and disclose the contents of the private communications of its customers and other authorized and unauthorized users only:

(i) to the extent necessary to render the service, and to maintain and protect the availability, integrity and confidentiality of the system; or

Commentary to Standard 2-8.1(b)(i)

This provision gives public providers the authority to acquire, disclose and use private communications in transmission through and storage with their service for essentially the same purposes as federal law does.\(^{218}\) Title III permits an “officer, employee or agent” of a provider to intercept, disclose and use wire and electronic communications “in the normal course of his employment while engaged in any activity which is

\(^{218}\) Concerning the meaning of “electronic storage” see the commentary to Standard 2-8.2(a)(ii) and (iii). Note that until the enactment of the USA PATRIOT Act, Title III equated stored wire communications with wire communications still in transmission, thus placing the same restrictions on an electronic communication service provider’s acquisition, disclosure and use of the contents of a stored wire communication as it did on the provider’s interception, disclosure and use of a wire communication obtained while still in transmission. However, as a result of the enactment of § 29 of the USA PATRIOT Act, a wire communication in electronic storage is no longer considered a “wire communication” for Title III purposes, and a service provider may now acquire, use and disclose the contents of a stored wire communication under the same provisions applicable to a stored electronic communication. See the commentary to Standard 2-8.1(a). Note, however, that § 209 of the USA PATRIOT Act “sunsets” on December 31, 2005. USA PATRIOT Act, § 224.
a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service," 18 U.S.C. 2511(2)(a)(i). 219 See the commentary to Standard 2-8.1(a). The Electronic Communications Privacy Act allows a communication service provider access to wire and electronic communications in electronic storage without any limitation, 18 U.S.C. § 2701(c), and permits a provider to disclose the contents of a wire or electronic communication while in such storage "as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service." 18 U.S.C. § 2702(b)(5). 220

Using different language, Standard 2-8(b)(i) authorizes a public provider to acquire, use and disclose private communications—aural and non-aural, while in transmission or in storage—"to the extent necessary to render the service, and to maintain and protect the availability, integrity and confidentiality of the system." This language is taken from the Guidelines for the Security of Information Systems developed by the Organization for Economic Cooperation and Development ("OECD"). The Guidelines define "availability" as "the characteristic of data and information being accessible and usable on a timely basis in the required manner"; "confidentiality" as "the characteristic of data and information disclosed only to authorized persons, entities and processes at authorized times and in the authorized manner"; and "integrity" as

219. Concerning the interception of communications "incident to the rendition of [a provider's] service, see, e.g., United States v. Ross, 713 F.3d 389 (8th Cir. 1983) (Title III not violated by inadvertent interception of communication by telephone company employee performing normal duties). For other examples, see 1 Carr, The Law of Electronic Surveillance (2000), at 3-70-3-71. Concerning the interception of communications "incident . . . to the protection of the rights or property of the provider of that service," see, e.g. United States v. Auler, 539 F.2d 642 (7th Cir. 1976) (proper for telephone company to intercept communications of suspected illegal users of telephone service and to disclose information about the intercepted communications to law enforcement agencies); United States v. Shah, 371 F.Supp. 1170 (D.C. W.D. Pa. 1974) (same). See, generally, Carr, supra, at 3-71, et seq.

220. 28 U.S.C. § 2702(b)(4) also permits disclosure of the contents of a stored wire or electronic communication "to a person employed or authorized or whose facilities are used to forward such communication to its destination," but such disclosure also seems "necessarily incident to the rendition of the service" within the meaning of § 2702(5). See Senate Report No. 99-541, 1986 U.S. Code, Cong. & Admin. News 3555, 3591-92 (noting that business procedures "necessary for the efficient operation of the communications system are included in the § 2511(2)(a) exemption as well as the exemptions [of subsection (b) of § 2702] relating to the disclosure of the message to the forwarding facilities and the exemption for service provider activities designed to protect the system and perform the service."
"the characteristic of data and information being accurate and complete and the preservation of accuracy and completeness." Given the threat hackers pose to the infiltration of even the largest and most sophisticated public communication service providers, the need to protect the availability, confidentiality and integrity of communications transmitted over their facilities is substantial. However, the means by which they do so should not unduly interfere with the reasonable expectation of privacy users of those systems are entitled to enjoy. Accordingly, a service provider should have no greater access to the communications of their users than is necessary for these purposes.

Consideration was given to permitting public service providers to monitor communications for one more purpose: "to protect the provider from liability for the conduct of its customers and other authorized and unauthorized users." However, in the interest of the privacy of authorized users, this authority was not included. Given its omission, a service provider should not be subjected to strict liability for harm to others caused by the conduct of a user of the service based on the failure of the provider to monitor or otherwise acquire, use and disclose the contents of the user's communications. If, of course, the service provider gains actual knowledge of wrongdoing by a user, liability for a failure to take appropriate action may result. See Standard 2-8.1(b)(iii) (permitting a public service provider to disclose to a law enforcement officer the contents of a private communication of a user of its service if the communication "appears to pertain to the commission of a crime").

(ii) in the case of a stored communication:
   (A) to the sender or an intended receiver of the communication, or an agent of the sender or an intended receiver; or
   (B) with the consent of the sender or an intended receiver of the communication; or

Commentary to Standard 2-8.1(b)(ii)

Subsection (ii) of Standard 2-8.1(b), unlike its other subsections, is concerned only with the disclosure of communications that are stored with a service provider. It has no application, as the other subdivisions do, to communications being transmitted by such a provider. Under federal law, a person or entity providing electronic communication service to the public may divulge the contents of a stored electronic communication "to an addressee or intended recipient of such communication or an
agent of such addressee or intended recipient,” 18 U.S.C. § 2702(b)(1), or “with the lawful consent of the originator or an addressee or intended recipient of such communication, 18 U.S.C. § 2702(b)(3). Someone to whom a copy of a communication is directed is both an “intended recipient” and an “addressee” within the meaning of Standard 2-8.1(b)(ii), and the omission of the term “addressee” is stylistic only.

Federal law also permits a person or entity providing electronic communication service to the public to divulge the contents of any electronic communication “while in transmission on that service” to any person “other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient,” 18 U.S.C. § 2511(3)(a), “with the lawful consent of the originator or any addressee or intended recipient of such communication.” 18 U.S.C. § 2511(3)(b)(ii). While the Standards do not include a comparable provision concerning the consensual disclosure by a communication service provider of a communication “while in transmission,” if the originator or an addressee consented to the disclosure, the communication would not be a “private communication” within the meaning of Standard 2-2.1(b), and thus its interception and disclosure by the service provider would not be prohibited by the Standards.

(iii) to a law enforcement officer:

(A) if otherwise authorized by these standards, or

Commentary to Standard 2-8.1(b)(iii)(A)

This provision is derived from 18 U.S.C. § 2511(b)(i), which permits a person or entity providing electronic communication service to the public to divulge the contents of an electronic communication while it is in transmission when such disclosure is “otherwise authorized in section 2511(2)(a) [which concerns the disclosure and use of intercepted wire, oral and electronic communications] or 2517 [which concerns the interception, disclosure and use of wire and electronic communications by providers of wire and electronic communication services],” and 18 U.S.C. § 2702(b)(2), which likewise permits a person or entity providing electronic communication service to the public to divulge the contents of a stored electronic communication “as otherwise authorized in section 2517, 2511(2)(a), or 2703 [concerning governmental access to the contents of electronic communications stored with a provider].”
In a similar fashion, Standard 2-8.1(b)(iii)(A) permits disclosure to law enforcement when such disclosure is otherwise authorized by these Standards. For example, Standard 2-4.16 sets forth the conditions for the disclosure and use of intercepted private communications; Standard 2-8.1(a) authorizes the interception, disclosure and use of private communications by a private service provider "for any lawful purpose," and Standard 2-8.1(b)(ii) authorizes the disclosure of a stored communication to, or with the consent of, the sender or intended receiver.

(B) if the public electronic communication service provider obtained the contents of the communication in a manner permitted by these standards, or obtained them inadvertently, and the communication appears to pertain to the commission of a crime.

Commentary to Standard 2-8.1(b)(iii)(B)

See also Standard 2-8.2(a), which, paralleling this provision, permits a law enforcement officer "to receive the contents of a private communication from an electronic communication service provider when: (1) the communication is evidence of a crime and was lawfully acquired by the provider." Because this provision permits a service provider, without court order or other authority, to disclose communications to law enforcement if the contents "appear to pertain to the commission of a crime," care must be taken to assure that the communications were obtained either lawfully or inadvertently, and not on a pretense designed to avoid the requirements applicable to such disclosures.

The comparable language of 18 U.S.C. § 2511(b)(iv) permits a person or entity providing electronic communication service to the public to divulge to law enforcement the contents of an electronic communication "inadvertently obtained by the service provider" while the communication was in transmission, if the contents "appear to pertain to the commission of a crime." Similarly, 18 U.S.C. § 2702(b)(6) permits a person or entity to divulge the contents of a stored communication "to a law enforcement agency, if such contents—(A) were inadvertently obtained by the service provider; and (B) appear to pertain to the commission of a crime." Language was added in Standard 2-8.1(b)(iii)(B) permitting the disclosure of criminal communications when the contents of the communication were obtained "in a manner permitted by these standards." The addition is designed to preclude the argument
that communications intentionally intercepted in a manner permitted by these Standards—for example, when “necessary to render the service, and to maintain and protect the availability, integrity and confidentiality of the system,” within the meaning of Standard 2-8.1(b)(i)—are not obtained “inadvertently.”

As part of its new anti-terrorist legislation, Congress recently amended 18 U.S.C. § 2702 to authorize an electronic communication service provider to disclose the contents of a stored communication of a subscriber “if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person requires disclosure of the information without delay.”221 This authority is broader than that provided in 18 U.S.C. 2702(b)(6) and Standard 2-8.1(b), each of which permit disclosure of the contents of a stored communication to law enforcement when the “communication appears to pertain to the commission of a crime,” since the disclosure authorized by this new provision may be made to someone outside of law enforcement, and because it applies to emergency situations whether or not they involve the commission of a crime. The Standards were adopted before this new provision was enacted, and contain no comparable provision.

Standard 2-8.2. Communications received by law enforcement from an electronic communication service provider

(a) A law enforcement officer should be permitted to receive the contents of a private communication from an electronic communication service provider when:

(i) the communication is evidence of a crime and was lawfully acquired by the provider;

Commentary to Standard 2-8.2(a)(i)

See Standard 2-8.1(b)(iii)(B), which permits an electronic communication service provider to disclose a private communication that “appears to pertain to the commission of a crime” if the service provider obtained

---

221. 18 U.S.C. § 2702(b)(6)(C), added by USA PATRIOT Act of 2001, § 212. Congress did not, however, make a comparable amendment to 18 U.S.C. 2511(2)(a), which governs the authority of a communication service provider to intercept, disclose or use the contents of wire and electronic communications obtained while still in transmission. Note that this provision “sunset” on December 31, 2005. USA PATRIOT Act, § 224.
the communication “in a manner authorized by these standards, or obtained them inadvertently.” Under either circumstance, the communication would be “lawfully acquired” by the provider within the meaning of this provision. This provision is not limited, however, to the disclosure of criminal communications to law enforcement by public providers, and applies also to such disclosures by “an electronic communication service provider not offering its service to the public,” which Standard 2-8.1(a) permits “to acquire, use and disclose the contents of the private communications transmitted over or stored with its service for any lawful purpose.” See the commentary to that provision.

(ii) the communication has been in storage with the provider, either temporarily and incidental to its transmission, or for purposes of its backup protection, and is obtained pursuant to a search warrant directing the provider to disclose the communication based on the application of an appropriate law enforcement official establishing probable cause to believe that the communication constitutes evidence of a crime; or

(iii) the communication has been in storage with the provider for more than 45 days, either temporarily and incidental to its transmission, or for purposes of its backup protection, and is obtained pursuant to a trial, grand jury or administrative subpoena authorized by federal or state law, or pursuant to a court order issued upon the application of a prosecuting attorney establishing reasonable grounds to believe that the contents of the communication are relevant and material to an ongoing criminal investigation.

**Commentary to Standard 2-8.2(a)(ii) and (iii)**

Under federal law, if a public or private electronic communication service provider has maintained a wire or electronic communication in "electronic storage" for 180 days or less, a governmental entity can obtain disclosure of its contents from the provider only pursuant to a search warrant based upon probable cause. 18 U.S.C. 2703(a).\footnote{222. Until recently, federal law treated the acquisition of stored wire communications like the interception of wire communications still in transmission, for which an electronic surveillance order is necessary. See the commentary to Standard 2-2.1(a). Because the Standards make no distinction between aural and non-aural communications, see Standard 2-3.1(a)(iv), stored private communications that include the human voice are afforded no more protection than those that do not.}
communication has been stored for more than 180 days, a prosecutor may also obtain it by a search warrant, but has the alternative of using instead an administrative subpoena, a grand jury subpoena, a trial subpoena, or a court order. 18 U.S.C. 2703(b). For this purpose, "electronic storage" is defined as "(A) any temporary, intermediate storage of [an] .... electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. 2510(17). Although a search warrant may be obtained without notice to the subscriber or customer of the service, subpoenas and court orders do require prior notice, but the notice may be postponed if the exigencies of the investigation require it.

The Standards do not include a definition of "electronic storage," but subdivisions (ii) and (iii) are similarly applicable to a communication that "has been in storage with the provider, either temporarily and incidental to its transmission, or for purposes of its backup protection." Under federal law and under the Standards, two problems arise in determining whether a communication is in "electronic storage." The first is determining when storage of a communication is "incidental" to its transmission. It might be argued that once a message is opened by its recipient, if the recipient does not immediately delete it from the service provider's server, and instead leaves it there as a convenient place for storing it for subsequent reference, it is no longer in storage temporarily or incidentally to its transmission. If, on the other hand, the recipient leaves the message on the server because he or she has not yet completed reading it, or digested its contents, its storage arguably continues to be temporary and incidental. While the recipient might achieve the same result by downloading the communication to the computer's hard drive or to a disk, few users of electronic communication service providers are likely to expect that leaving the communication on the server for a short period of time significantly diminishes the reasonableness of their expectation of privacy in it. Moreover, inexpensive devices are now available that do not give users the alternative of downloading or printing out communications they receive, and they

223. Even if the storage of a communication on a server were to be deemed no longer incidental to its transmission once the communication was first opened, technological problems could arise in determining when that defining event had occurred, particularly given that electronic communication service providers frequently offer features to their users permitting them to mark and treat opened mail as if it had not been opened.
may retain access to them only by keeping them on the server. For such users, when a communication is no longer stored temporarily and incidental to its transmission is even more difficult to determine.

The second problem arises from the fact that "electronic storage" of a communication includes not only the storage incidental to its transmission, but also to storage by a provider "for purposes of backup protection of such communication." Storage for this purpose can and often does last beyond the recipient's deletion of the communication from the server, and to the extent that it does, the period of time the provider retains the contents of a communication is beyond the recipient's control. Moreover, some providers maintain the communications they transmit in backup storage longer than others, and few users are likely to know how long any one provider stores its communications for backup purposes.

Both of these problems may be somewhat alleviated as public awareness grows concerning these matters. With time, those who use electronic communication services should be better informed concerning the practical and legal consequences of leaving communications in "temporary" storage with the provider of the service they use. And service providers should more prominently disclose how long they keep the communications their users transmit in backup storage, and should carefully consider—and explain to their subscribers and customers—why that long a period of backup storage is necessary.

However these problems are resolved, the question remains where to draw the line between when probable cause and a search warrant should be required for law enforcement to obtain the contents of a stored communication, and when a subpoena or a court order should suffice. Congress drew the line at 180 days based upon its view that when a person stores an electronic communication with a service provider for a substantial period of time, "the communication service provider is no longer really acting in the capacity of medium-of-communication like the Postal service; rather its real function diminishes to that of a third-party custodian of the customer's records. . . ."224 The Justice Department reported to the Task Force on Technology and Law Enforcement that there have been few, if any, cases in which it has sought to obtain the contents of a communication more than 180 days after it was transmitted. After much debate, Standard 2-8.2(a) draws the line at 45 days rather than 180, reasoning that when a communication has been stored more than 45 days, it has taken on a degree of concreteness and permanence.

far removed from its origin as an ephemeral electronic transmission. The difference is not likely to have practical importance since few service providers maintain private communications in “electronic storage” for more than 45 days, let alone for 180.

Standard 2-8.2(a)(iii) provides that a court order requiring a service provider to disclose the contents of a stored communication may be “issued upon the application of a prosecuting attorney establishing reasonable grounds to believe that the contents of the communication are relevant and material to an ongoing criminal investigation.” This provision is taken from 18 U.S.C. 2703(d), which permits such an order to issue if a “governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication . . . are relevant and material to an ongoing criminal investigation.”

(b) When an application for a search warrant is made pursuant to Standard 2-8.2(a)(ii), the applicant should be required to inform the judge from whom the warrant is sought of any previous applications made by or known to the applicant for a warrant requiring the disclosure of stored communications of the same customer.

Commentary to Standard 2-8.2(b)

Although a search warrant issued pursuant to Standard 2-8.2(a)(i) requires a demonstration of probable cause to believe that a crime is being committed and that the stored electronic communications will contain evidence of that crime, many other requirements for an application for an electronic surveillance order authorizing the contemporaneous interception of the same communications do not apply. For example, the applicant would not have to demonstrate that conventional means of investigation had been exhausted before the search warrant could issue, and the application would not have to be made by an attorney or authorized by a politically accountable public official. A law enforcement officer unable to satisfy the additional requirements necessary for an electronic surveillance order could apply instead for a series of search warrants and thus obtain the electronic communications transmitted by an electronic communication service provider for the account of a particular customer shortly after they had been transmitted and while they were stored with the provider. If the search warrants were issued with sufficient frequency, the intrusion on the privacy of the
senders and receivers of those communications would be the essentially the same as if they had been obtained contemporaneously with their transmission. Thus, Standard 2-8.2(b) requires that a judge to whom application is made for a search warrant authorizing the disclosure of stored electronic communications be told of prior applications relating to the same customer, so that the judge is appropriately informed in exercising his or her discretion in determining whether to issue the warrant sought.

(c) When an electronic communication service provider discloses private communications to a law enforcement officer:
   (i) the law enforcement agency to which the disclosure is made should be required to give prior notice of the disclosure to the customer if the disclosure is made pursuant to a trial, grand jury or administrative subpoena, or pursuant to a court order, provided that a court may postpone such notice upon a showing of good cause; and
   (ii) based upon a showing of good cause, a court may prohibit the provider from notifying the customer of the disclosure.

Commentary to Standard 2-8.2(c)

Like 18 U.S.C.§ 2703(b), Standard 2-8.2(b)(i) requires that when an electronic communication service provider discloses the contents of a communication, the law enforcement agency must give prior notice to the customer of the disclosure, if the disclosure is made pursuant to a trial, grand jury or administrative subpoena, or pursuant to a court order. As under federal law, such prior notice is not required if the contents of the communication were obtained by search warrant.

Under both Standard 2-8.2(b)(i) and § 2703(b), the required notice may be postponed for good cause. Standard 2-8.2(b)(i) does not specify what "good cause" must be shown, but the federal statute, which requires reason to believe that a specific "adverse result" may result from giving notice of the court order or subpoena, see 18 U.S.C. 2705(a)(1)(A) and (B), provides appropriate examples. The "adverse result[s]" specified are: "(A) endangering the life or physical safety of an individual; (B) flight from prosecution; (C) destruction or tampering with evidence; (D) intimidation of potential witnesses; or (E) otherwise seriously jeopardizing an investigation or unduly delaying a trial." 18 U.S.C. 2705(a)(2). When the contents of a communication are disclosed pursuant to a court order, § 2705(a)(1)(A) requires that the post-
ponement of notice come from the judge who orders the disclosure, but when the contents of a communication are disclosed pursuant to a subpoena, § 2705(a)(1)(B) permits notice to be delayed based "upon the execution of a written certification of a supervisory official." Standard 2-8.2(b)(i), however, requires for both a subpoena and court order that the showing be made to a judge, who may then order the postponement.

Like 18 U.S.C. § 2705(b), Standard 2-8.2(b)(ii) provides that upon a showing of good cause, a court may prohibit an electronic communication service provider from notifying a customer of the existence of the court order or subpoena. As for postponing notice from law enforcement, Standard 2-8.2(b)(ii) does not specify what "good cause" must be shown for such an order, but federal law again provides appropriate examples by requiring that the same showing of a possible "adverse result" be made as would be necessary to postpone notice of the disclosure by a government entity. See 18 U.S.C. § 2705(b). Although § 2705(b) also permits an order to be issued prohibiting a provider from disclosing to a customer the existence of a search warrant, Standard 2-8.2(b)(ii) contains no such provision. Consistent with the Standards, however, an applicant for a search warrant may also seek such a prohibition for good cause shown.

(d) Upon the written request of a law enforcement officer or prosecuting attorney, an electronic communication service provider should be required to take all necessary steps to preserve a record of the contents of a stored electronic communication pending the issuance of a court order or subpoena. If such a request is made, the provider should be required to preserve the record for ninety days. Upon a renewed written request by the prosecuting attorney, the provider should be required to preserve the record for an additional ninety days.

Commentary to Standard 2-8.2(d)

This provision is designed to permit a law enforcement officer or a prosecuting attorney to require that an electronic communication service provider preserve the contents of a stored communication while a court order is being sought or a subpoena is being obtained. In some cases, if such preservation were not required, the contents of a communication could be lost before it was obtained by law enforcement, because the customer deleted it from the provider's service and/or because the provider
removed it from backup storage. See the commentary to Standard 2-8.2(a)(ii). Federal law provides comparable authority. See 18 U.S.C. § 2703(f), which states that "[a] provider of wire or electronic communication services . . . upon request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process," and 18 U.S.C. § 2704, which permits a governmental entity to "include in its subpoena or court order a requirement that the service provider . . . create a backup copy of the contents of the electronic communications sought in order to preserve those communications."

(e) A law enforcement officer should be permitted to disclose, receive or use the contents of a private communication which the officer has obtained from an electronic communication service provider by means authorized by these standards, or evidence derived therefrom, only to the extent it is in the proper performance of the officer's official duties.

Commentary to Standard 2-8.2(d)

This provision parallels Standard 2-4.16(a), which provides that "[a] law enforcement officer should be permitted to disclose, receive or use the contents of a private communication intercepted by means of electronic surveillance conducted in a manner authorized by these Standards, or evidence derived therefrom, only to the extent it is the proper performance of the officer's official duties." This provision applies, however, to the disclosure, receipt and use of private communications obtained from an electronic surveillance communication service provider.

Standard 2-8.3. Communications received by other persons from an electronic communication service provider.

A person who is not a law enforcement officer:
(a) should be prohibited from obtaining from an electronic communication service provider the contents of a private communication stored with that provider unless disclosure of that communication by the provider to that person is permitted by these standards or is otherwise lawful; and
(b) should be permitted to disclose or use the contents of such a communication if the person obtains the contents of the communication lawfully and uses or discloses it for any lawful purpose.

Commentary to Standard 2-8.3

Subsection (a) of this Standard provides that a person who is not a law enforcement officer should be prohibited from receiving from an electronic communication service provider that which the provider may not properly disclose to it. Subsection (b) of this Standard is adapted from Standard 2-4.16(b), which similarly provides that any person who is not a law enforcement officer should be permitted to disclose or use a private communication intercepted by means of electronic surveillance conducted in a manner authorized by these Standards "if the person obtains the contents of the communication lawfully and uses or discloses it for any lawful purpose."