ELECTRONIC SURVEILLANCE MANUAL

PROCEDURES and CASE LAW

FORMS

Revised June 2005
(complete in one volume)

FOREWORD

This manual was prepared by the Electronic Surveillance Unit, Office of Enforcement Operations, Criminal Division, and is designed primarily to assist federal prosecutors and investigative agents in the preparation of electronic surveillance applications made pursuant to Title 18, United States Code, Sections 2510-2522 (2001)("Title III") and associated statutes. It is not intended to confer any rights, privileges, or benefits upon defendants, nor does it have the force of a United States Department of Justice directive. See United States v. Caceres, 440 U.S. 741 (1979). In addition to outlining and discussing the statutory requirements of Title III applications, this manual also sets forth the Department's authorization process, provides guidance in filing Title III pleadings before the court, and discusses the applicable case law as well as both novel, and frequently arising, legal issues involved in Title III litigation. Samples of the most commonly filed pleadings follow the text.

INTRODUCTION

This manual sets forth the procedures established by the Criminal Division of the Department of Justice to obtain authorization to conduct electronic surveillance pursuant to Title 18, United States Code, Sections 2510-2522 (2001)(Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended by the Electronic Communications Privacy Act of 1986 (ECPA), the Communications Assistance for Law Enforcement Act of 1994 (CALEA), the Antiterrorism and Effective Death Penalty Act of 1996 (Antiterrorism Act)), the USA-Patriot Act of 2001, and the Homeland Security Act of 2002 and discusses the statutory requirements of each of the pleadings. Throughout this manual, the above federal wiretap statutes will occasionally be referred to collectively as "Title III."

This manual is divided into two sections. The first section provides an overview of the procedures to follow when applying for authorization to conduct electronic surveillance, and discusses format, statutory and policy requirements, and pertinent case law concerning specific electronic surveillance issues. The second section provides sample forms pertaining to electronic surveillance involving wire, oral and electronic communication interceptions, pen register/trap and trace procedures, access to transactional data and stored wire and electronic communications, and the use of tracking devices. These forms are intended only to provide general guidance in drafting the most frequently used pleadings and do not prohibit alternative approaches.

TABLE OF CONTENTS

I. THE ELECTRONIC SURVEILLANCE UNIT 1

II. TITLE III AUTHORIZATION PROCESS 1

III. THE ELECTRONIC SURVEILLANCE PLEADINGS 3
1. The Application 3
2. The Affidavit 7
3. The Order 15

IV. ELECTRONIC COMMUNICATIONS 16
1. Coverage under Title III 16
2. Stored Electronic Communications - 18 U.S.C. § 2703 16

V. EXTENSION AND SPINOFF APPLICATIONS 19
1. Extension Applications 19
2. Spinoff Applications 21

VI. ROVING INTERCEPTIONS 22
1. Roving Oral Interception 23
2. Roving Wire or Electronic Interception 24

VII. EMERGENCY PROCEDURES 24
1. Title III Interceptions 24
2. Pen Register/Trap and Trace Devices 26
3. How to Contact the ESU 27

VIII. PROGRESS REPORTS 27

IX. SEALING 27
1. Overview 27
2. When to Seal 28
3. Sealing Delays 29
4. How to Seal/Custody of the Tapes 30
5. Suppression for Failure to Seal Properly 30
6. Resealing 31

X. INVENTORY NOTICE 31

XI. DISCLOSURE OF TITLE III EVIDENCE 32
1. 18 U.S.C. § 2517(1), (2), (6), (7), (8) - Use and Disclosure of Interception Information 32

2. 18 U.S.C. § 2517(3) - Testimonial Use 34
3. 18 U.S.C. § 2517(4) - Privileged Communications . . 35
4. 18 U.S.C. § 2517(5) - Use of "Other Crimes" Evidence 35

XII. DISCOVERY 36
1. 18 U.S.C. § 2518(9), 2518(10)(a) 36
2. The Federal Rules 37

XIII. PEN REGISTERS/TRAPS AND TRACES 38

XIV. CELL SITE SIMULATORS/DIGITAL ANALYZERS/TRIGGERFISH . . 40

XV. THE LEGAL AUTHORITIES REQUIRED TO LOCATE CELLULAR TELEPHONES 41

XVI. MOBILE TRACKING DEVICES 48

XVII. VIDEO SURVEILLANCE 48

XVIII. CONSENSUAL MONITORING 50
1. Consensual Monitoring by Law Enforcement 50
2. Consensual Monitoring by Private Parties 51

XIX. CUSTODIAL MONITORING 52
1. Law Enforcement Access to Monitored Prison Calls . 52
2. Case Law on Custodial Monitoring 54

Samples

Application for Wire and/or Oral Interceptions 56

Affidavit for Oral and/or Wire Interception 63

Order for Interception of Wire and/or Oral Communications . . 72

Order to Service Provider 77

Sample Minimization Instructions
for Oral and Wire Communications 79

Application for Electronic Communications Interception . . . 85

Affidavit for Electronic Communications Interception 90

Order for Interception of Electronic Communications 99

Sample Title III Roving Affidavit 103

Application for Approval of Emergency Interception of Wire, Oral or Electronic Communications Under 18 U.S.C. 2518(7) . . 137

Affidavit in Support of Application for Approval of Emergency Interception of Wire, Oral or Electronic Communications Under 18 U.S.C. 2518(7) 143

Order Approving Emergency Interception of Wire, Oral or Electronic Communications Under 18 U.S.C. 2518(7) . . . 153

Application for Sealing 157

Order for Sealing 160

Application for 2703(d) Court Order 162

2703(d) Court Order 164

Application for Trap and Trace/Pen Register 166

Order for Trap and Trace/Pen Register 168

Application for Order Permitting Government To Use Its Own Pen Register/Trap and Trace Equipment (Triggerfish/Digital Analyzer or Similar Device 171

Order Permitting Government To Use Its Own Pen Register/Trap and Trace Equipment (Triggerfish/Digital Analyzer or Similar Device) 173

Combined 3123/2703 Application 175

Combined 3123/2703 Order 189

Application for Video Surveillance 197

Order for Video Surveillance 201

Application for Disclosure 204

Order for Disclosure of Interceptions 207

Section 2517(5) Application for Testimonial Use of Interceptions Relating to "Other Offenses" 209

Section 2517(5) Order Permitting Testimonial Use of Interceptions Relating to "Other Offenses" 212

Inventory Application 214

Order for Inventory 216

Inventory Notice 218

Application for Destruction of Tapes 219

Order for Destruction of Tapes 222

Affidavit for Mobile Tracking Device 224

Order for Mobile Tracking Device 227

I. THE ELECTRONIC SURVEILLANCE UNIT

The Electronic Surveillance Unit (ESU) operates within the Office of Enforcement Operations (OEO), Criminal Division, and handles all requests made pursuant to Title III to conduct non-consensual, domestic surveillance of wire, oral, and electronic communications for law enforcement purposes. The ESU does not handle state wiretaps or requests to conduct domestic national security electronic surveillance pursuant to the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. §§ 1801, et seq.)(FISA). Questions concerning FISA taps should be directed to the Office of Intelligence and Policy Review at (202) 514-5600.

Attorneys in the ESU are responsible for reviewing and processing all Title III requests, and are available to assist in the preparation of Title III applications and to answer questions on any Title III-related issue. All such inquiries should be directed to (202) 514-6809. ESU attorneys will also provide assistance in responding to suppression motions and preparing briefs on Title III issues. For assistance in this area, contact the Chief or Deputy Chief of the ESU at the above number.

II. TITLE III AUTHORIZATION PROCESS

The following is a brief explanation of the Department of Justice's procedures for reviewing and authorizing Title III applications.

1. A copy of the proposed order, application, and affidavit is submitted to the ESU and to the Washington, D.C., office of the investigative agency handling the case. Those pleadings should be sent to the Office of Enforcement Operations, Electronic Surveillance Unit, 1301 New York Avenue, N.W., 12th Floor, Washington, D.C. 20005, and should be sent via overnight mail. If the documents are short enough, they may be faxed directly to the ESU at (202) 616-8256. For security reasons, these pleadings may not be sent via e-mail.

Except in the case of genuine emergencies, discussed below, most original applications require approximately one week to review and process from the time the ESU receives the affidavit. Spinoff requests (i.e., applications to conduct electronic surveillance at a new location or over a new facility that are related to an ongoing or previously conducted interception reviewed by the ESU) are considered original applications and are reviewed and processed in the same manner described below, and require agency approval. Extension requests (i.e., applications

to continue interceptions over the same facility or premises) require review only by the ESU, and not the investigative agency. Because the ESU is presently reviewing approximately 1,700 Title III applications per year, it is imperative when coordinating an investigation or planning extension requests that sufficient time is allowed for the Title III application to be reviewed by both the ESU and, when appropriate, the investigative agency.

2. When an application is received in the ESU, it is logged in and assigned to one of the reviewing attorneys. This attorney will be responsible for reviewing all spinoffs and extensions arising from the original application. The attorney will discuss with the Assistant United States Attorney (AUSA) handling the case any necessary changes or additions to the affidavit, and will coordinate the processing of the request with the investigative agency's Office of Legal Counsel or, in the case of the FBI, the appropriate section within the Criminal Investigative Division. Once the affidavit has been reviewed by both the ESU attorney and the investigative agency's counsel and is in final form, the head of the investigative agency will send, through the ESU, a memorandum to the Assistant Attorney General (or Acting Assistant Attorney General) for the Criminal Division requesting that electronic surveillance be authorized in this case. Because it is the investigative agency that has the ultimate responsibility for conducting the requested electronic surveillance, the ESU cannot recommend approval of a Title III until this agency memorandum has been finalized. (The agency memorandum is required only for original applications and spinoff applications involving a new facility or location; it is not required for an extension request.) Minor changes or additions to the affidavit can usually be faxed to the ESU and the investigative agency for insertion in the original; however, in those cases when an affidavit needs substantial revision, a new copy must be submitted. Generally, an AUSA's only contact person will be the ESU attorney assigned to the case. Any problems or changes requested by the investigative agency's counsel will be communicated to the affiant by the agency after consultation with the ESU attorney.

3. After reviewing the application, the ESU attorney will write an action memorandum to the Assistant Attorney General (AAG), Criminal Division, summarizing and analyzing the relevant facts and legal issues as they pertain to the proposed electronic surveillance, and discussing the application's compliance with the statutory requirements of Title III. This memorandum also contains the ESU's recommendation of approval or disapproval of the application. Once the reviewing attorney has written the action memorandum, a package is prepared containing the

memorandum and the pleadings. This package, together with the requesting memorandum from the head of the investigative agency, is then sent to the AAG's office for final review and authorization.

4. If the application is authorized, the ESU will fax the AUSA the following items: the authorization document, which is a memorandum from a properly designated official to the Director of OEO, authorizing the application for Title III surveillance, and a copy of the Attorney General's most recent delegation order, which identifies those individuals to whom the Attorney General has delegated authority to authorize Title III applications. The designated official's authorization memorandum and the copy of the Attorney General's delegation order should be filed with the pleadings.

III. THE ELECTRONIC SURVEILLANCE PLEADINGS

Discussed below are the requirements for each of the three documents comprising a Title III application: the Application, the Affidavit, and the Order. These requirements, which are set forth in 18 U.S.C. § 2518, are applicable to requests for oral, wire and electronic communications. Samples of each of these pleadings are found in the Forms section.

1. The Application

a. It must identify the applicant (an AUSA) as a law enforcement or investigative officer, and must be in writing, signed by the AUSA and made under oath. 18 U.S.C. § 2518(1). It must be presented to a federal district court or court of appeals judge, and be accompanied by the Department's authorization memorandum signed by an appropriate Department of Justice official. See 18 U.S.C. §§ 2516(1) and 2510(9)(a); In re United States, 10 F.3d 931 (2d Cir. 1993)(explaining that "judge of competent jurisdiction" does not include magistrate judges), cert. denied sub nom. Korman v. United States, 513 U.S. 812 (1994).

b. It must identify the type of communications to be intercepted. 18 U.S.C. § 2518(1)(b)(iii). "Wire communications" are "aural transfers" (involving the human voice) that are transmitted, at least in part by wire, between the point of origin and the point of reception, i.e., telephone calls. 18 U.S.C. § 2510(1). This includes voice communications conducted over cellular telephones, cordless telephones and voice pagers, as well as over traditional landline telephones. "Oral communications" are only treated as such by Title III when they

involve utterances by a person exhibiting a reasonable expectation of privacy, such as conversations within a person's residence, private office, or car. 18 U.S.C. § 2510(2). An "electronic communication" most commonly involves digital display paging devices and electronic facsimile machines, but also includes electronic mail and computer transmissions. It does not include communications made through tone-only paging devices, communications from a tracking device, or electronic funds transfer information. 18 U.S.C. § 2510(12).

c. It must identify the specific federal offenses for which the affidavit sets forth probable cause to believe have been, are being, or will be committed. 18 U.S.C. § 2518(1)(b)(I). The offenses that may be the predicates for a wire or an oral interception order are limited to those set forth in 18 U.S.C. § 2516(1). In the case of electronic communications, a request for interception may be based on any federal felony, pursuant to 18 U.S.C. § 2516(3).

d. It must provide a particular description of the nature and location of the facilities over which, or the place where, the interception is to occur. 18 U.S.C. § 2518(1)(b)(ii). Specifically excepted from the particularity requirement of 18 U.S.C. § 2518(1)(b)(ii) are the roving interception provisions set forth in 18 U.S.C. § 2518(11). See also 18 U.S.C. § 2518(12). The specific requirements of the roving provisions are discussed in detail below. Briefly, in the case of a roving oral interception, the application must show, and the order must state, that it is impractical to specify the locations where the oral communications of a particular named subject or subjects are to be intercepted. 18 U.S.C. § 2518(11)(a)(ii), (iii). In the case of a roving wire or electronic interception, the application must show, and the order must find, that there is probable cause to believe that the actions of the particular named subject (or subjects) could have the effect of thwarting interception from a specified facility. 18 U.S.C. § 2518(11)(b)(ii), (iii). In the case of a roving interception, the accompanying DOJ authorization document must be signed by an official at the Assistant Attorney General or acting Assistant Attorney General level or higher. 18 U.S.C. § 2518(11)(a)(I), (b)(I).

e. It must identify the person(s), if known, committing the offenses and whose communications are to be intercepted. 18 U.S.C. § 2518(1)(b)(iv); United States v. Donovan, 429 U.S. 413 (1977). It is the Department's policy to name in the pleadings all persons as to whom there is probable cause to believe are committing the offenses ("violators"), and then to delineate who among the violators will be intercepted over the target

facilities discussing the offenses ("interceptees"). (Typically, the list of interceptees is nothing more than a subset of the larger list of violators.) It is also Department policy to name individuals in Title III pleadings even if their involvement does not rise to the level of probable cause. See United States v. Ambrosio, 898 F. Supp. 177 (S.D.N.Y. 1995) ("since nothing in the statute restricts the government from naming in the affidavit individuals as to whom it may not have probable cause, the statute's goal of providing [inventory] notice [of the wiretap pursuant to 18 U.S.C. § 2518(8)(d)] is actually furthered by naming more, rather than fewer, persons"). See also United States v. Martin, 599 F.2d 880 (9th Cir.), cert. denied, 441 U.S. 962 (1979)(same).

f. It must contain a statement affirming that normal investigative procedures have been tried and failed, or are reasonably unlikely to succeed, or are too dangerous to employ. 18 U.S.C. § 2518(1)©. The applicant may then state that a complete discussion of attempted alternative investigative techniques is set forth in the accompanying affidavit.

g. It must contain a statement affirming that the affidavit contains a complete statement of facts concerning all previous applications that have been made to intercept the oral, wire, or electronic communications of any of the named persons or involving the target facility or location. 18 U.S.C. § 2518(1)(e); United States v. Bianco, 998 F.2d 1112 (2d Cir. 1993)(holding that the duty to disclose prior applications covers all persons named in the application and not just those designated as "principal targets"), cert. denied, 511 U.S. 1069 (1994); United States v. Ferrara, 771 F. Supp. 1266 (D. Mass. 1991)(when "the government has decided to name in its Application individuals believed to be co-conspirators of the proposed principal targets of an interception order, it has an obligation to inform the issuing judge of all prior requests for authority to intercept communications of those individuals").

h. If involving an oral (and occasionally a wire or an electronic) interception, it must contain a request that the court issue an order authorizing investigative agents to make surreptitious and/or forcible entry to install, maintain, and remove electronic interception devices in or from the targeted premises. In effecting this, the applicant should notify the court as soon as possible after each surreptitious entry.

I. If involving a wire interception (and an electronic interception involving, for example, a facsimile machine), it must contain a request that the authorization apply not only to

the target telephone number, but to any changed telephone number subsequently assigned to the same cable, pair, and binding posts used by the target landline telephone within the thirty (30) day interception period. With regard to cellular telephones, the language should read:

IMSI/ESN Combo

The authorization given is intended to apply not only to the target telephone numbers listed above, but to any other telephone numbers or telephones accessed through the international mobile subscriber identification (IMSI) number used by the one target cellular telephone, to any other IMSI numbers accessed through that target cellular telephone number, and to any other telephone numbers subsequently assigned to the instrument bearing the same electronic serial number as the other target cellular telephone, within the thirty-day period. The authorization is also intended to apply to the target telephone numbers referenced above regardless of service provider, and to background conversations intercepted in the vicinity of the target telephones while the telephones are off the hook or otherwise in use.

ESN

The authorization given is intended to apply not only to the target telephone number listed above, but to any other telephone number subsequently assigned to the instrument bearing the same electronic serial number used by the target cellular telephone within the thirty-day period. The authorization is also intended to apply to the target telephone number referenced above regardless of service provider, and to background conversations intercepted in the vicinity of the target telephone while the telephone is off the hook or otherwise in use.

See United States v. Duran, 189 F.3d 1071 (9th Cir. 1999)(Title III order remained valid when cell phone MIN change was followed by an ESN change a few days later); United States v. Baranek, 903 F.2d 1068, 1071-72 (6th Cir. 1990)(aural version of the "plain view" doctrine applied).

j. If involving a wire (and sometimes an electronic) interception, it must also contain a request that the court issue an order directing the service provider, as defined in 18 U.S.C. § 2510(15), to furnish the investigative agency with all information, facilities, and technical assistance necessary to facilitate the ordered interception. 18 U.S.C. §§ 2511(2)(a)(ii) and 2518(4). The application should also request that the court order the service provider and its agents and employees not to

disclose the contents of the court order or the existence of the investigation. 18 U.S.C. § 2511(2)(a)(ii).

k. It should contain a request that the court's order be issued for a period not to exceed thirty (30) days, measured from the earlier of the day on which the interception begins or ten (10) days after the order is entered, and that the interception must terminate upon the attainment of the authorized objectives. 18 U.S.C. § 2518(1)(d), (5).

l. It should contain a statement affirming that all interceptions will be minimized in accordance with Chapter 119 of Title 18, United States Code, as described further in the affidavit.

m. It should disclose any plans to use civilian monitors in the execution of the order. U.S. v. Lopez, 300 F.3d 46 (1st Cir. 2002).

2. The Affidavit

a. It must be sworn and attested to by an investigative or law enforcement officer, as defined in 18 U.S.C. § 2510(7). Department policy precludes the use of multiple affiants except in rare circumstances. (When the use of multiple affiants is deemed appropriate by the ESU, it must be indicated clearly which affiant swears to which part of the affidavit, or that each affiant swears to the entire affidavit.) If a state or local law enforcement officer is the affiant for a federal electronic surveillance affidavit, he must be deputized as a federal officer of the agency with responsibility for the offenses under investigation. See 18 U.S.C. § 2516(1)(interceptions are to be conducted by the federal agency responsible for the offenses for which the application is made); United States v. Lyons, 695 F.2d 802 (4th Cir. 1982)(judge was aware that state and local law enforcement officials were part of a DEA task force and that they would be monitoring the wire under the supervision of the DEA, the federal agency ordered to conduct the interception). Section 2518(5) permits non-officer "Government personnel" or individuals acting under contract with the government to monitor conversations pursuant to the interception order. These individuals must be acting under the supervision of an investigative or law enforcement officer authorized to conduct the interception when monitoring communications, and the affidavit should note the fact that these individuals will be used as monitors pursuant to section 2518(5). The First Circuit holds that the government must disclose in the application its intention to use civilian monitors in the execution of the order.

U.S. v. Lopez, 300 F.3d 46 (1st Cir. 2002). Civilian Department of Defense personnel would appear to qualify as "Government personnel" and could, therefore, without deputization, assist in the Title III monitoring process (e.g., as translators), if such assistance does not violate the Posse Comitatus laws ("PCA"), 10 U.S.C. § 375 and 18 U.S.C. § 1385, and related regulations, 32 C.F.R. § 213.10(a)(3), (7). An opinion issued by the Office of Legal Counsel ("OLC"), Department of Justice, dated April 5, 1994, concluded that such assistance by military personnel would not violate the PCA. The OLC analysis did not extend to National Guard personnel, who are considered state employees rather than Federal Government personnel. Consequently, use of members of the National Guard will require that they be deputized as law enforcement officers or placed under contract. A copy of the OLC opinion may be obtained from the ESU. See generally United States v. Al-Talib, 55 F.3d 923 (4th Cir. 1995); United States v. Khan, 35 F.3d 426 (9th Cir. 1994); United States v. Yunis, 924 F.2d 1086 (D.C. Cir. 1991); Hayes v. Hawes, 921 F.2d 100 (7th Cir. 1990).

b. It must identify the subjects, describe the facility or location that is the subject of the proposed electronic surveillance, and list the alleged offenses.

c. It must establish probable cause that the named subjects are using the targeted telephone(s) or location(s) to facilitate the commission of the stated offenses.

Any background information needed to understand the instant investigation should be set forth briefly at the beginning of this section. The focus, however, should be on recent and current criminal activity by the subjects, with an emphasis on their use of the target facility or location to facilitate this activity. This is generally accomplished through information from an informant, cooperating witness, or undercover agent, combined with pen register information or other telephone records for the target telephone, or physical surveillance of the target premises. It is Department policy that pen register or telephone toll information for the target telephone, or physical surveillance of the target premises, standing alone, is generally insufficient to establish probable cause.

Probable cause to establish criminal use of the facilities or premises requires independent evidence of use in addition to pen register or surveillance information, e.g. informant or undercover information. (It is preferable that all informants used in the affidavit to establish probable cause be qualified according to the "Aguilar-Spinelli" standards (Aguilar v. Texas,

378 U.S. 108 (1964) and Spinelli v. United States, 393 U.S. 410 (1969)), rather than those set forth in the more recent Supreme Court decision of Illinois v. Gates, 463 U.S. 1237 (1983). On rare occasions, criminal use of the target facilities or premises may be established by an extremely high volume of calls to known or suspected coconspirators or use of the premises by them that coincides with incidents of illegal activity. It is Department policy that the affidavit reflect use of the target telephone or premises within twenty-one days of the date on which the Department authorizes the filing of the application. The subjects' use of the target facilities or premises within the twenty-one-day period may be evidenced through pen register information and/or physical surveillance that updates earlier use. Historical information (i.e., information older than six months from the date of the application), combined with pen register information or physical surveillance alone, is generally insufficient to establish probable cause. Pen register information and physical surveillance not only serve to update the probable cause as to the criminal use of a telephone or premises, but also are required (in the absence of other information) to establish the need for the proposed electronic surveillance by demonstrating what types of criminal communications are expected to be intercepted over the telephone or within the premises during the thirty-day authorization period.

d. It must explain the need for the proposed electronic surveillance and provide a detailed discussion of the other investigative procedures that have been tried and failed, are reasonably unlikely to succeed, or are too dangerous to employ in accomplishing the goals of the investigation. It need not be shown that no other normal investigative avenues are available, only that they have been tried and proven inadequate or have been considered and rejected for the reasons described. There should also be a discussion as to why electronic surveillance is the technique most likely to succeed. When drafting this section of the affidavit, the discussion of other investigative techniques should be augmented with facts particular to the specific investigation and subjects. General declarations about the exhaustion of alternative techniques will not suffice. It is most important that this section be tailored to the facts of the specific case and be more than a recitation of boilerplate language. The affidavit must discuss the particular problems involved in the investigation in order to fulfill the requirement of section 2518(1)©. It should explain specifically why investigative techniques, such as physical surveillance or the use of informants and undercover agents, are inadequate in the particular case. For example, if physical surveillance is

impossible or unproductive because the suspects live in remote areas or will likely be alerted to law enforcement's presence, the affidavit should set forth those facts clearly. If the informants refuse to testify or cannot penetrate the hierarchy of the criminal organization involved, the affidavit should explain why that is the case in this particular investigation. If undercover agents cannot be used because the suspects deal only with trusted associates, the affidavit must so state and include the particulars. It is not enough, for example, to state that the use of undercover agents is always difficult in organized crime cases because organized crime families, in general, deal only with trusted associates. While the affidavit may contain a general statement regarding the impossibility of using undercover agents in organized crime cases, it must also demonstrate that the subject or subjects in the instant case deal only with known associates. The key is to tie the inadequacy of a specific investigative technique to the particular facts underlying the investigation. U.S. v. Canales-Gomez, 358 F.3d 1221 (9th Cir. 2004) (Judge Stephen Trott, former Assistant Attorney General of the Justice Department's Criminal Division, authored a Ninth Circuit opinion reversing a district court's "necessity"-based suppression of wiretap evidence in a major drug conspiracy case. "We are unable to discern anything missing from the affiant's affidavit, and we see nothing in it that justifies the district court's characterization of any part of it as 'boilerplate.' A judicially-imposed requirement that the government attempt to use all potential informants before securing a wiretap would be impractical and contrary to investigatory experience and the force of our precedent. The government need not prove that informants would be totally useless." Trott's opinion is comprehensive and unequivocal in its holding that the agent's Title III affidavit contained a full and complete statement of the facts and that the necessity for the wiretap was clearly established in light of the government's interest in establishing the full scope of the conspiracy, the added difficulty, expense and danger involved in the use of informants to investigate and prosecute persons engaged in clandestine criminal activity, and the critical role wiretap evidence plays in corroborating informant testimony and in ensuring that what investigators are told by the informants is accurate. See also U.S. v. Fernandez, 388 F.3d 1199 (9th Cir. 2004)(recognizing the "common sense approach" to the necessity issue adopted by the Ninth Circuit in Canales-Gomez); United States v. Aviles, 170 F.3d 863 (9th Cir. 1998) (DEA agent working on task force with FBI agent had a duty to disclose to the FBI agent all information material to the FBI agent's application for a wiretap); United States v. Blackmon, 273 F.3d 1204 (9th Cir. 2001)(wiretaps suppressed because government failed to make a particularized showing of necessity);

United States v. London, 66 F.3d 1227 (1st Cir. 1995)(the government must make "a reasonable good faith effort to run the gamut of normal investigative procedures before resorting to" electronic surveillance), cert. denied, 116 S. Ct. 1542 (1996); United States v. Mondragon, 52 F.3d 291 (10th Cir. 1995)(because the affidavit contained no alternative investigative need statement, the evidence was suppressed); United States v. Ashely, 876 F.2d 1069 (1st Cir. 1989)("conclusory statements that normal investigative techniques would be unproductive, based solely on an affiant's prior experience, do not comply with the requirements of section 2518(1)©"); United States v. Santora, 600 F.2d 1317 (9th Cir. 1979)(evidence was suppressed because the government failed to show exhaustion of alternative investigative techniques for each new facility to be tapped).

e. It must contain a full and complete statement of any prior electronic surveillance involving the persons, facilities, or locations specified in the application. 18 U.S.C. § 2518(1)(e). This statement should include the date, jurisdiction, and disposition of previous applications, as well as their relevance, if any, to the instant investigation. In addition to any known prior applications, the agency conducting the investigation should run an "ELSUR" check of its own electronic surveillance indices, the indices of any other participating agency, and the indices of any agency which would likely have investigated the subjects in the past. In narcotics investigations, it is the Department's policy that the Drug Enforcement Administration, the Federal Bureau of Investigation, and the United States Customs Service conduct an ELSUR check to determine if any prior related electronic surveillance has been conducted.

f. It must contain a statement of the period of time for which the interception is to be maintained. 18 U.S.C. § 2518(1)(d). Section 2518(5) provides that an order may be granted for no longer than is necessary to achieve the objectives of the investigation, or in any event no longer than thirty (30) days, whichever occurs first. The statute further provides that the thirty-day period begins on either the day on which investigative officers first begin to conduct the interception or ten days after the order is entered, whichever is earlier. This ten-day grace period is intended primarily for the installation of oral monitoring equipment (microphones), allowing investigators time to break and enter, if necessary, and set up the equipment before the thirty-day period begins to be calculated. This provision may also be used when delays arise in installing monitoring devices used in wire or electronic interceptions. In either case, the provision is not intended to

provide an additional ten-day start-up period on a regular basis throughout the investigation; any delays that are encountered should be real and defensible if challenged. Accordingly, the ten-day grace period would normally apply only to the initial installation of equipment and should not be invoked in the following circumstances: 1) when an extension order has been obtained and the equipment has remained in place; 2) for an original application when the equipment has already been installed; or 3) in wire or electronic interception cases when a pen register or other device permitting almost immediate access to the target facility is already in place. The time will then run from the earlier of the day on which the interceptions begin (the time at which the monitoring equipment is installed and activated), or ten days after the order is entered. With extension applications, because the monitoring equipment is already in place and can be easily activated, the thirty-day period should be calculated from the date and time the order is signed. Because of conflicting court decisions regarding the counting of the thirty-day period for purposes of Title III interceptions, the supervising attorney should ensure that the method of computing time is set forth in the court order and made known to monitoring personnel. See United States v. Gangi, 33 F. Supp.2d 303 (S.D.N.Y. 1999)(counting calendar days rather than 24-hour periods, unless order provides otherwise) and United States v. Smith, 223 F.3d 554 (7th Cir. 2000)(Fed.R.Crim.P. 45, minus weekend and holiday exception, applies.) Notwithstanding the method used, communications should not be intercepted for longer than a strict counting of thirty days.

g. It must contain a statement affirming that monitoring agents will minimize all interceptions in accordance with Chapter 119 of Title 18, United States Code, as well as other language addressing any specific, anticipated minimization problems, such as the interception of privileged attorney-client communications, or conversations in a foreign language or code. 18 U.S.C. § 2518(5); United States v. Scott, 436 U.S. 128 (1978)(minimization efforts must be objectively reasonable); United States v. London, 66 F.3d 1227 (1st Cir. 1995)(three factors should be considered to determine whether minimization was reasonable: 1) the nature and complexity of suspected crimes; 2) the government's efforts to minimize; and 3) the degree of supervision by the judge), cert. denied, 116 S. Ct. 1542 (1996).

If any of the named subjects are facing pending state or federal criminal charges, these persons and the nature of their pending charges should be identified in the affidavit, and both the minimization language in the affidavit and the instructions given to the monitoring agents should contain cautionary language

regarding the interception of privileged attorney-client conversations. The essential elements of the attorney-client privilege are: 1) the client sought legal advice; 2) the advice was sought from an attorney acting in his professional capacity; 3) the communication between the attorney and the client was for the purpose of seeking legal advice; and 4) the communication was made in confidence. United States v. Gotti, 771 F. Supp. 535 (E.D.N.Y. 1991). The privilege is not available if a non-privileged third party is present during the conversation, or if the content of the communication is disclosed to such a third party, or if the communication was made for the purpose of committing a crime. Gotti, supra. See also United States v. Johnston, 146 F.3d 785 (10th Cir. 1998); United States v. Bankston, 2000 WL 1252582 (E.D. La.); United States v. Abbit, 1999 WL 1074015 (D. Or.).

If a monitor intercepts a privileged attorney-client conversation, the monitor should make a notation of that conversation on the log and notify the supervising attorney, who should advise the judge. The tape of the conversation should be sealed and no disclosure of that conversation should be made to other investigative officers. See United States v. Noriega, 764 F. Supp. 1480 (S.D. Fla. 1991)(tapes were first screened by an agent unconnected with the case; if the tapes contained attorney-client communications, the agent was to seal the tapes immediately and segregate them from the rest; if only part of the tape contained attorney-client conversations, then a sanitized copy of it would be provided to the case agents and prosecuting attorneys). If the interception of attorney-client conversations is inadvertent and the government acted in good faith, then only the privileged conversations will be suppressed. See also United States v. Ozar, 50 F.3d 1440 (8th Cir.), cert. denied, 116 S. Ct. 193 (1995).

If any of the named subjects speak a foreign language or converse in code, the statute permits after-the-fact minimization of wire and oral communications when an expert in that code or foreign language is not reasonably available to minimize the conversations contemporaneously with their interception. In either event, the minimization must be accomplished as soon as practicable after the interception. 18 U.S.C. § 2518(5). Such after-the-fact minimization can be accomplished by an interpreter who listens to all of the communications after they have been recorded and then gives only the pertinent communications to the agent. See United States v. David, 940 F.2d 722 (1st Cir.)("by translating only the portions of the tapes that seemed relevant, the government's actions comported with the expectations of Congress"), cert. denied, 502 U.S. 989 (1991); United States v.

Gambino, 734 F. Supp. 1084 (S.D.N.Y. 1990)(an interpreter need not be on constant duty; efforts to hire more translators had failed).

After-the-fact minimization is a necessity for the interception of electronic communications such as cell phone or pager text messages, facsimile transmissions, and internet transmissions such as e-mail and images. In such cases, all communications are recorded and then examined by a monitoring agent and/or a supervising attorney to determine their relevance to the investigation. Disclosure is then limited to those communications by the subjects or their confederates that are criminal in nature. See United States v. Tutino, 883 F.2d 1125 (2d Cir. 1989)("because it is impossible to tell from the clone beeper whether a conversation even took place, much less the content of any conversation that might have taken place, traditional minimization requirements do not apply"), cert. denied, 493 U.S. 1081 (1990). The Ninth Circuit held that in the Title III investigation of the Montana Freemen, the minimization procedures employed for the interception of facsimiles (electronic communications) were adequate under the circumstances. The Title III order required that:

> Each facsimile transmission will be printed on the machine used to intercept facsimile transmissions. The monitoring agent and [assistant United States attorney] will decide, based on the identities of the sender and recipient and the subject matter of the transmission, whether the facsimile appears to be pertinent to the criminal offenses listed in the court's order. If the facsimile does not appear to be pertinent, the intercepted transmission will be placed in an envelope and sealed. It will then be placed in a locked drawer until it is turned over to the court with the other intercepted transmissions after the interception order has expired.

The ECPA and Title III do not require that the government mimic conversational minimization procedures by skipping lines in a fax and then continue reading line by line. Citing Scott v. U.S., 436 U.S. 128 (1978) and the ECPA's legislative history, the court said: "We interpret Congress's 'common sense' idea of electronic minimization to mean that law enforcement in some circumstances may look at every communication. Congress intended that the pool of investigative material be filtered. Here the district court established a reasonable procedure to eliminate irrelevant information. Under the circumstances, that is all the ECPA and Title III require. U.S. v. McGuire, 307 F.3d 1192 (9th Cir. 2002).

Finally, when communications are intercepted that relate to any offense not enumerated in the authorization order, the monitoring agent should report it immediately to the AUSA, who should notify the court at the earliest opportunity. Approval by

the issuing judge should be sought for the continued interception of such conversations. An order under 18 U.S.C. § 2517(5) may have to be obtained for testimonial use of "other offense" information.

h. When the request is to intercept a cellular or otherwise mobile telephone (i.e., a car, or otherwise portable, telephone) or a portable paging device, or to install a microphone in an automobile, the affidavit should contain a statement that, pursuant to 18 U.S.C. § 2518(3), the interceptions may occur not only within the territorial jurisdiction of the court in which the application is made, but also outside that jurisdiction (but within the United States). Because these devices are easily transported across district lines, this language should be used if there is any indication that the target telephone, paging device, or vehicle will be taken outside the jurisdiction of the court issuing the electronic surveillance order. The order should specifically authorize such extra-jurisdictional interceptions, and should be sought in the jurisdiction having the strongest investigative nexus to the object in which the monitoring device is installed. See United States v. Ramirez, 112 F.3d 849 (7th Cir. 1997).

3. The Order

The authorizing language of the order should mirror the requesting language of the application and affidavit, and comply with 18 U.S.C. § 2518(3), (4), and (5). In short, the order must state that there is probable cause to believe that the named violators are committing particular Title III predicate offenses (or, in the case of electronic communications, any federal felony); that the named interceptees have used, are using, and/or will use the target facility or premises (described with particularity) in furtherance thereof; that particular communications concerning the predicate offenses will be obtained through the requested interception; and that normal investigative techniques have been tried and have failed, or are reasonably unlikely to succeed if tried, or are too dangerous to employ. The court will then order that the agents of the investigative agency are authorized to intercept the communications over the described facility or at the described premises for a specific length of time, and that the interception must be conducted in such a way as to minimize the interception of communications not otherwise subject to interception. The court may also mandate that the government make periodic progress reports, pursuant to 18 U.S.C. § 2518(6). In the case of a roving interception, the court must make a specific finding that the requirements of 18 U.S.C. § 2518(11) have been demonstrated adequately. Any other

special circumstances, such as extra-jurisdictional interception in the case of mobile interception devices (pursuant to 18 U.S.C. § 2518(3)) or surreptitious entry should also be authorized specifically in the order. An order to seal all of the pleadings should also be sought at this time. 18 U.S.C. § 2518(8)(b).

The government should also prepare for the court a technical assistance order to be served on the communication service provider. 18 U.S.C. §§ 2511(2)(a)(ii) and 2518(4). This is a redacted order that requires the service provider to assist the agents in effecting the electronic surveillance.

IV. ELECTRONIC COMMUNICATIONS

1. Coverage under Title III

One of the primary changes effected by ECPA was the addition of electronic communications to the types of communications, in addition to oral and wire, whose interception is regulated by Title III. An "electronic communication" is one in which the human voice is not used in any part of the communication. 18 U.S.C. § 2510(12). The types of electronic communications that are most commonly the subject of Title III applications are those occurring over digital-display paging devices, electronic facsimile machines and the internet. Applications for these types of interceptions must comply with the requirements set forth in section 2518. Unlike applications to intercept oral or wire communications, section 2516(3) provides that any attorney for the government may authorize an application to be made to intercept electronic communications. By agreement with Congress, however, prior Department approval is required for most applications to conduct interceptions of electronic communications. On February 1, 1991, an exception was made for electronic communications intercepted over digital-display pagers; applications involving digital-display pagers may be authorized by an Assistant United States Attorney. This exception applies only to interceptions involving electronic communications to digital-display pagers. Department approval is still required as a prerequisite to filing an application for an interception order targeting any other form of electronic communication (e.g., facsimile transmissions, cell phone text messages, e-mail, and computer transmissions).

2. Stored Electronic Communications - 18 U.S.C. § 2703

In addition to the changes to numerous provisions of Title III, ECPA also defined and regulated government access to various

new forms of electronic communications, including stored electronic communications and transactional records.

a. Under 18 U.S.C. § 2703(a), the government may require a service provider to disclose the contents of an electronic or wire communication that is in electronic storage[1] in an electronic communications system[2] for one hundred and eighty days or less, only pursuant to a search warrant. (As defined in 18 U.S.C. § 2510(8), "'contents', when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication.") If the information has been in electronic storage for more than one hundred and eighty days, disclosure may be required by a search warrant (without prior notice to the subscriber), a court order sought pursuant to section 2703(d) (with prior notice to the subscriber, requirements for this order are summarized below), or an administrative, grand jury, or trial subpoena (with prior notice to the subscriber). Delayed notice to the subscriber may be sought under section 2705.

Under section 2703(b), the government may obtain the contents of any electronic communication held in a remote

---

"Electronic storage" is defined in 18 U.S.C. § 2510(17) as: "(A) any temporary, intermediate storage of a wire or 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." To illustrate "incidental to ... transmission," consider the example of electronic mail. If electronic mail has been sent but not opened by the intended recipient, then it is in "electronic storage ... incidental to ... transmission." Once the electronic mail has been opened by the recipient, it can be argued that the electronic mail is no longer in electronic storage incidental to transmission.

An "electronic communication service provides its users the ability to send or receive wire or electronic communications." S. Rep. No. 541, 99th Cong., 2d Sess. 14 (1986). Examples of electronic communication services would be telephone companies (such as Verizon) and electronic mail companies (such as America On Line). Id. Verizon serves as an electronic communication service when it facilitates the placement of telephone calls, and America On Line does, as well, when it transmits electronic mail from the sender to the recipient.

computing service[3] by way of a search warrant, an administrative, grand jury, or trial subpoena, or a court order authorized by section 2703(d), with a request seeking delayed notice to the subscriber/customer pursuant to section 2705. See Steve Jackson Games, Incorporated v. United States Secret Service, 36 F.3d 457 (5th Cir. 1994)(upheld use of search warrant to seize stored email on computer).

b. Under 18 U.S.C. § 2703(c)(2), an electronic communication service or remote computing service must disclose to a government entity the name; address; local and long distance telephone connection records, or records of session times and durations; length of service (including start date) and types of service utilized; telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and means and source of payment for such service (including any credit card or bank account number), of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under 2703(c)(1)(search warrant, court order under 2703(d), or the consent of the subscriber or customer). The requirements for obtaining a section 2703(d) court order must be met even if the government seeks the court order only to obtain subscriber and telephone information. Those requirements are that the government must offer "... specific and articulable facts showing that there are reasonable grounds to believe that ... the records or other information sought are relevant and material to an ongoing criminal investigation." Id.

As described in H. Rep. No. 647, 99th Cong., 2d Sess. 23 (1986), remote computer services allow "persons [to] use the facilities of these services to process and store their own data." The House Report further explains that "[a] subscriber or customer to a remote computing service transmits records to a third party, a service provider, for the purpose of computer processing. This processing can be done with the customer or subscriber using the facilities of the remote computing service in essentially a time-sharing arrangement, or it can be accomplished by the service provider on the basis of information supplied by the subscriber or customer." Id. America On Line (AOL) would function as a remote computing service when the recipient of an electronic mail transmission decides to save the transmission on AOL's system.

c. Pursuant to 18 U.S.C. § 2703(f)(Supp. 1996), a service provider or remote computing service, upon the request of a governmental entity, must preserve records and other evidence in its possession pending the issuance of a court order or other process.

For additional information concerning stored electronic communications, contact the Computer Crime and Intellectual Property Section at (202) 514-1026.

V. EXTENSION AND SPINOFF APPLICATIONS

1. Extension Applications

Applications to continue previously authorized electronic surveillance for an additional period, usually another thirty days, may be made at or near the expiration of the previous thirty-day order. (If, for scheduling reasons, an extension application must be filed before the end of an ongoing thirty-day period, the new thirty-day period is calculated from the date of the extension order.) As long as the investigation is continuing, subsequent applications to continue interceptions over the same facility or at the same location, and involving substantially the same subjects and offenses are considered extensions. See United States v. Plescia, 48 F.3d 1452 (7th Cir.), cert. denied, 116 S. Ct. 114 (1995); United States v. Carson, 969 F.2d 1480 (3d Cir. 1992). As noted above, extension applications require Department authorization, but are reviewed only by the ESU and not the investigative agency. An exception occurs when the electronic surveillance has been inactive for more than thirty days; in these instances, the Department requires that a new memorandum requesting renewed electronic surveillance be submitted by the head of the investigative agency.

The tapes should be sealed at the end of each interception period, especially if the investigation is lengthy and definitely whenever there is any time gap between extensions. While the statute requires the tapes to be sealed at the "expiration of the period of the order, or extensions thereof," the appellate courts have differed on the amount of time that may elapse between orders before the new order is no longer considered an extension, and, thus, necessitating sealing under the statute. If there is a sealing delay, a good reason for the delay must be provided and a showing made that the defendant was not prejudiced by the failure to seal in a timely fashion. See United States v. Ojeda-Rios, 495 U.S. 257 (1990)(Title 18, United States Code, Section

2518(8)(a) requires the court to presume prejudice if the sealing requirements are not met).

An extension affidavit follows the same format and carries the same statutory requirements as does the affidavit that supported the original application. 18 U.S.C. § 2518(5). The primary difference is in the probable cause section, which must focus on the results obtained (or lack thereof) during the most recent interception period, including any new information regarding the subjects' recent use of the targeted facilities or premises. 18 U.S.C. § 2518(1)(f). The affidavit should incorporate by reference the original and all previous extension applications, and then discuss in a paragraph or two the progress of the investigation to date and summarize new information obtained during the past thirty days. If no relevant interceptions were made during the previous period, a sufficient explanation must be provided to the court (for example, technical or installation problems with monitoring equipment, or the physical absence of the subject during all or part of the interception period), along with a reasonable, factually based explanation of why the problems are expected to be rectified during the next thirty days. Id. A sampling of recent interceptions sufficient to establish probable cause that the subjects are continuing to use the targeted facilities or location in furtherance of the stated offenses should then be described. The affidavit should not contain verbatim transcripts or a series of pieced-together progress reports; rather, selected and paraphrased or highlighted portions of a few key, criminal conversations should be set forth, along with an explanation, if necessary, of the context in which the conversations were spoken, and the affiant's opinion (based on his/her training and experience) of their meaning if they are in code or are otherwise unclear. The excerpted conversations should reflect results obtained over the bulk of the thirty-day period, and not consist solely of interceptions obtained, for example, during the first ten days. The most recent excerpt of an intercepted communication should be, if possible, within seven calendar days of when the Title III application is submitted to the Criminal Division for approval. If there are no recent interceptions, the affidavit should include a brief explanation as to why that is the case.

Other changes from the original application will be in the "Need for Interception and Alternative Investigative Techniques" section, which should state that the facts set forth in the original affidavit regarding the exhaustion of alternative investigative techniques are continuing, citing examples of what additional efforts have been made during the preceding

interception period, and explaining why the electronic surveillance conducted thus far has been insufficient to meet the goals of the investigation. It is also frequently necessary to add or delete subjects and offenses due to new information learned from the interceptions. If any additional subjects are added, an ELSUR check needs to be done for their names.

Finally, Title III does not limit the number of extension affidavits that may be filed. United States v. Vazquez, 605 F.2d 1269 (2d Cir.), cert. denied, 444 U.S. 981 (1979); United States v. Ruggiero, 824 F. Supp. 379 (S.D.N.Y. 1993). If the objective of the intercept is to determine a conspiracy's scope and to identify its participants, more extensive surveillance may be justified. United States v. Nguyen, 46 F.3d 781 (8th Cir. 1995); United States v. Earls, 42 F.3d 1321 (10th Cir. 1994), cert. denied, 514 U.S. 1085 (1995). In addition, interceptions need not terminate because some targets have been arrested. United States v. Wong, 40 F.3d 1347 (2d Cir. 1994), cert. denied, 116 S. Ct. 190 (1995).

The ESU can usually review and process these applications in three to four days, depending upon the caseload of the attorney assigned to the case. If it is important that the electronic surveillance not be interrupted between orders, the extension request should be submitted to the ESU with sufficient lead time.

2. Spinoff Applications

As stated above, new applications arising from the same investigation to conduct electronic surveillance over additional facilities are considered original requests, even though the same subjects are targeted, and are reviewed and processed by both the ESU and the investigative agency as such. A new facility is one which, in the case of landline telephones, is carried over a different cable, pair, and binding posts, or, in the case of cellular telephones, over an instrument bearing a different electronic serial number and telephone number than that of the originally authorized facility. Thus, for example, a targeted landline telephone that is given a new telephone number during an interception period, but which maintains the same location (the same cable, pair, and binding posts) is not considered a spinoff, and applications for additional thirty-day interception periods are extensions of the original authorization. If this situation occurs and the subject of the electronic surveillance obtains a new number for the telephone during the course of the monitoring, the court should be notified.

As with extension requests, prior affidavits in the same investigation may be incorporated by reference, obviating the need to set forth anew all of the facts that established the original probable cause; the probable cause section in the spinoff application should focus on the newly targeted facility or location, and any additional subjects. As noted above, if new subjects are added, an ELSUR check must be done for their names.

A spinoff application may not, however, merely incorporate by reference the "Need for Interception and Exhaustion of Alternative Techniques" section of the original affidavit. This section must address the facts as they apply to the spinoff application. See United States v. Santora, 600 F.2d 1317 (9th Cir. 1979)(evidence was suppressed because the spinoff affidavit incorporated by reference the original affidavit's showing of inadequacy of normal investigative procedures; spinoff affidavits require a showing of the difficulties of employing normal investigative techniques with regard to the new telephone, premises and subjects); U.S. v. Castillo-Garcia, 117 F.3d 1179 (10th Cir. 1997)("Even with 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 to consider whether normal investigative procedures could be used effectively, particularly in light of any evidence obtained as a result of each succeeding wiretap.").

The minimization language of the original affidavit should also be reviewed to ensure that it comports with any new facts particular to the new facility or location.

VI. ROVING INTERCEPTIONS

ECPA established the "roving" provisions of Title III. See 18 U.S.C. § 2518(11), (12). These provisions permit the interception of oral, wire, or electronic communications of named subjects without requiring that a specific facility or premises be identified in advance of the authorization. The roving provisions are intended to be used infrequently, and only when the required elements have been fulfilled clearly. Authorization for a roving interception must be granted by a Department of Justice official at the Assistant Attorney General or Acting Assistant Attorney General level or higher.

In a roving interception, the requirements of 18 U.S.C. § 2518(1)(b)(ii), necessitating a particular description of the nature and location of the facilities from which or the place where the communications are to be intercepted, may be waived when, in the case of an oral interception, identification of a

specific premises prior to court authorization is not practical; and in the case of a wire or an electronic interception, when the actions of a particular subject could have the effect of thwarting interception from a specified facility. In each circumstance, the subject who is the target of a roving interception must be identified at the time the application is made and only those conversations in which the subject is a participant may be intercepted. Once the named subject is no longer a party to the conversation, the interception must cease, even though the conversation may be criminal in nature. In practice, it is helpful to remember that the authorization attaches to a specific subject, rather than to a particular facility or location.

As to roving interception of wire or electronic communications, the order must limit interceptions to such time as it is reasonable to presume that the target person is or was reasonably proximate to the instrument through which such communication will be or was transmitted. 18 U.S.C. § 2518(11)(b)(iv).

As to roving interception of oral communications, monitoring agents must ascertain a specific location before the interception of oral communications begins. 18 U.S.C. § 2518(12).

The ESU takes the position that if physical surveillance is not possible, spot monitoring may be employed to meet the requirements of sections 2518(11)(b)(iv) and 2518(12).

1. Roving Oral Interception

In the case of a roving oral interception, the application must establish, and the order must specifically find, that probable cause exists that a particular subject is committing a Title III predicate offense at locations that are not practical to specify. 18 U.S.C. § 2518(11)(a)(ii); United States v. Bianco, 998 F.2d 1112 (2d Cir. 1993), cert. denied, 511 U.S. 1069 (1994); United States v. Orena, 883 F. Supp. 849 (E.D.N.Y. 1995).

The impracticality element may be established by informant information showing that the named subject changes meeting places frequently and with little or no warning, usually in order to avoid law enforcement surveillance, combined with a pattern of physical surveillance over a period of weeks confirming that the subject does, in fact, meet at changing locations with little or no advance warning sufficient to permit prior identification of a targeted premises. While the amount and type of evidence available will vary with the particular circumstances of each

case, it is essential in all cases that enough factual background information be provided to support the court's finding that it is impractical to specify a particular location at the time the application is filed.

Because of the technical difficulties inherent in obtaining interceptions pursuant to a roving oral authorization, it is wise to check with the field and technical agents before time and resources are expended doing the preliminary fieldwork and drafting the affidavit. The statutory requirements for obtaining a roving oral interception order make actual execution of the order difficult: unless the roving oral interception is done in conjunction with an ongoing wiretap or with the benefit of up-to-the-minute information from an informant or undercover agent concerning the location of an impending meeting, it is usually technically impossible to effect the interceptions, because there is no time to install monitoring equipment before the meeting occurs. Sufficient advance notice of a specific location, however, argues in favor of targeting a particular location through a regular electronic surveillance order rather than using the roving provision. Thus, field agents should be required to present a practical and reasonably workable plan for installing the listening device prior to requesting a roving oral interception.

2. Roving Wire or Electronic Interception

In the case of a roving wire or electronic interception, 18 U.S.C. § 2518(11)(b)(ii) requires a probable cause showing that the actions of a named subject could have the effect of thwarting interception from a specified facility.

While the statute does not address the jurisdictional restrictions of a roving interception, the legislative history suggests, and Department policy concurs, that roving interception authorization is not transjurisdictional; orders must be obtained in each jurisdiction in which roving interceptions are to be conducted. However, in cases involving mobile cellular telephones or vehicles that cross jurisdictional lines, 18 U.S.C. § 2518(3), which permits extra-jurisdictional orders, would apply.

VII. EMERGENCY PROCEDURES

1. Title III Interceptions

Title 18, United States Code, Section 2518(7), permits the Attorney General (AG), the Deputy Attorney General (DAG), or the

Associate Attorney General (Assoc. AG) to specially designate any investigative or law enforcement officer to determine whether an emergency situation exists that requires the interception of wire, oral, or electronic communications pursuant to Title III before a court order can, with due diligence, be obtained. The statute defines an emergency situation as one involving an immediate danger of death or serious injury to any person, conspiratorial activities threatening the national security interest, or conspiratorial activities characteristic of organized crime. 18 U.S.C. § 2518(7). In all but the most unusual circumstances, the only situations likely to constitute an emergency are those involving an imminent threat to life, e.g., a kidnapping or hostage taking, or imminent terrorist activity. See Nabozny v. Marshall, 781 F.2d 83 (6th Cir.)(kidnapping and extortion scenario constituted an emergency situation), cert. denied, 476 U.S. 1161 (1986); United States v. Crouch, 666 F. Supp. 1414 (N.D. Cal. 1987)(wiretap evidence suppressed because there was no imminent threat of death or serious injury). Because the Federal Bureau of Investigation has jurisdiction over these offenses, the Bureau will likely be the requesting agency in an emergency.

The Criminal Division's emergency procedures require that before the requesting agency contacts the AG, the DAG, or the Assoc. AG, oral approval to make the request must first be obtained from the Assistant Attorney General (AAG) or a Deputy Assistant Attorney General (DAAG) of the Criminal Division. This approval is facilitated by the ESU, which is the initial contact for the requesting United States Attorney's Office and the agency. In practice, the emergency procedures are initiated when the AUSA in charge of the case contacts an ESU attorney. At the same time, the field agents contact their agency headquarters personnel. After discussions with both the AUSA and an agency headquarters representative, the ESU attorney, in consultation with the OEO Director or an Associate Director, determines whether the statutory requirements have been met. Both the ESU and the agency's headquarters must agree that an emergency situation and the means to implement the requested electronic surveillance exist. The ESU attorney then briefs the AAG or a DAAG and obtains oral authorization on behalf of the Criminal Division. The ESU attorney notifies the agency representative and the AUSA that the Division has approved the seeking of an emergency authorization. The appropriate agency representative (usually the Director or Deputy Director of the FBI) then contacts the AG, the DAG, or the Assoc. AG and seeks permission to make a determination that an emergency situation exists as defined in the statute.

Once the AG, the DAG, or the Assoc. AG authorizes the law enforcement agency to make the determination whether to proceed

with the emergency Title III, the government then has forty-eight hours (including weekends and holidays) from the time the authorization was obtained to apply for a court order approving the interception. The package submitted to the court will consist of the AUSA's application, the affidavit, and a proposed order. (This package must be reviewed by the ESU before it is submitted to the court.) The affidavit in support of the government's after-the-fact application to the court for an order approving the emergency interception must contain only those facts known to the AG, the DAG, or the Assoc. AG at the time the emergency interception was approved. The application must be accompanied by a written verification from the requesting agency noting the date and time of the emergency authorization. The government may request, at the time it files for court-authorization for the emergency, court-authorization to continue the interception beyond the initial forty-eight hour period. If continued authorization is sought at the same time, one affidavit may be submitted in support of the emergency application and the extension application, but the affidavit must clearly indicate which information was communicated to the AG, the DAG, or the Assoc. AG at the time the emergency interception was approved and which information was developed thereafter. Two separate applications and proposed orders (one set for the emergency and one set for the extension) should be submitted to the court. If the government seeks continued authorization, that application must be reviewed by the ESU and approved by the Criminal Division like any other Title III request would.

2. Pen Register/Trap and Trace Devices

Title 18, United States Code, Section 3125 permits the AG, the DAG, the Assoc. AG, any AAG, any Acting AAG, or any DAAG to specially designate any investigative or law enforcement officer to determine whether an emergency situation exists requiring the installation and use of a pen register or a trap and trace device before an order authorizing such installation and use can, with due diligence, be obtained. An emergency situation under this section exists if it involves the immediate danger of death or serious injury to any person, or conspiratorial activities characteristic of organized crime. Unlike the Title III emergency provision, under 18 U.S.C. § 3125, a situation involving conspiratorial activities threatening national security does not, in itself, constitute an emergency. The government has forty-eight hours after the installation has occurred to obtain a court order in accordance with section 3123 approving the installation or use of the pen register/trap and trace device. Failure to obtain a court order within this forty-eight-hour period shall constitute a violation of the pen register/trap and trace chapter.

As with an emergency Title III, the AUSA in charge of the case should contact the ESU to request an emergency pen register or trap and trace. After discussions with the AUSA, the ESU attorney, in consultation with the OEO Director or an Associate Director, determines whether the statutory requirements have been met. If so, the ESU attorney will contact the appropriate Criminal Division official and obtain authorization to proceed. Once that approval has been obtained, the ESU attorney will contact the AUSA and advise that the emergency use has been approved, and that the law enforcement agency may proceed with the installation and use of the pen register/trap and trace. The ESU attorney will send a verification memorandum, signed by the authorizing official, to the AUSA. The AUSA should submit this authorization memorandum with the application for the court order approving the emergency use.

3. How to Contact the ESU

If an emergency situation arises after regular business hours, an ESU attorney may be reached through the Department of Justice Command Center at (202) 514-5000. During regular business hours, the ESU may be reached at (202) 514-6809; fax - (202) 616-8256.

VIII. PROGRESS REPORTS

Title 18, United States Code, Section 2518(6) provides for periodic progress reports to be made at the judge's discretion. These are generally made at five-, seven-, or ten-day intervals, and should contain enough (summarized) excerpts from intercepted conversations to establish continuing probable cause and need for the surveillance. Any new investigative information pertinent to the electronic surveillance, such as newly identified subjects or the addition of new violations, should be brought to the court's attention in the progress reports, and then be included in the next extension request. See generally, United States v. Van Horn, 789 F.2d 1492 (11th Cir.), cert. denied, 479 U.S. 854 (1986); In re De Monte, 674 F.2d 1169 (7th Cir. 1982); United States v. Plescia, 773 F. Supp. 1068 (N.D. Ill. 1991).

IX. SEALING

1. Overview

Title 18, United States Code, Section 2518(8)(a) requires that the tape recordings of the intercepted conversations be sealed "[i]mmediately upon the expiration of the period of the order, or extensions thereof." The purpose of the sealing requirement is to preserve the integrity of the electronic surveillance evidence. Section 2518(8)(a) contains an explicit

exclusionary remedy for failure to comply with the sealing requirement: "[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 any...[electronic surveillance] evidence ... under subsection (3) of section 2517." This provision requires that the government explain not only why it failed to seal or why a delay in sealing occurred, but also why the failure or delay is excusable. See United States v. Ojeda-Rios, 495 U.S. 257 (1990); United States v. Carson, 52 F.3d 1173 (2d Cir. 1995), cert. denied, 116 S. Ct. 934 (1996).

2. When to Seal

As noted above, 18 U.S.C. § 2518(8)(a) requires that the tape recordings of the intercepted conversations be sealed "[i]mmediately upon the expiration of the period of the order, or extensions thereof." If the government does not seek an extension of the original order, then the tapes of the intercepted conversations must be sealed immediately upon the expiration of the original order. If an extension or several extension orders are obtained, then the tapes of the intercepted conversations must be sealed upon the expiration of the last extension order. The definition of an extension order is construed very narrowly, and applies only "whe[n] the surveillance involves the same telephone, the same premises, the same crimes, and substantially the same persons" as the original order. United States v. Gallo, 863 F.2d 185 (2d Cir. 1988), cert. denied, 489 U.S. 1083 (1989); United States v. Scafidi, 564 F.2d 633 (2d Cir. 1977), cert. denied, 436 U.S. 903 (1978).

When caused by administrative difficulties, a brief hiatus between the expiration of an order and the extension will not prevent the extension from being deemed an "extension" within the meaning of section 2518(8)(a). Thus, the obligation to seal will not arise until the termination of the final extension order. See United States v. Plescia, 48 F.3d 1452 (7th Cir. 1995), cert. denied, 116 S. Ct. 114 (1995); United States v. Carson, 969 F.2d 1480 (3d Cir. 1992); United States v. Nersesian, 824 F.2d 1294 (2d Cir.), cert. denied, 484 U.S. 957 (1987). Despite the statutory language and the case law, the Department recommends that the AUSA seal the tapes at the end of each extension order to ensure the integrity of each month's interceptions. It is better to seal immediately every thirty days than to have to explain months, or even years, later why the tapes were not sealed during some minimal gaps in the interception period, and hope that the court will find that the explanation is satisfactory (even when it is clear that the tapes have not been altered). See United States v. Jackson, 207 F.3d 910 (7th Cir. 2000)(government intended to obtain an extension order, but when

it became clear that there would be an indefinite delay in designing a new hidden microphone, the government sealed the tapes 32 days after the expiration of the order).

A spinoff order targeting a different facility is not an extension, even though it involves the same subjects or investigation. Accordingly, those tape recordings should be sealed as soon as that interception order expires when no extension is contemplated. Each spinoff should likewise be compartmentalized.

3. Sealing Delays

The Second Circuit holds that a sealing delay of more than two days requires the government to provide a satisfactory explanation for violating the "immediate" sealing requirement of section 2518(8)(a). See United States v. Pitera, 5 F.3d 624 (2d Cir. 1993), cert. denied, 510 U.S. 1131 (1994); United States v. Wong, 40 F.3d 1347 (2d Cir. 1994).

When the issuing judge is unavailable, that circumstance will likely constitute a satisfactory explanation for a slightly extended sealing delay. United States v. Williams, 124 F.3d 411 (3d Cir. 1997)(substitute judge directed that tapes be sealed on Monday following Friday termination of surveillance); United States v. Maxwell, 25 F.3d 1389 (8th Cir.)(judge scheduled the sealing for seven days after termination), cert. denied, 513 U.S. 1031 (1994); United States v. Pedroni, 958 F.2d 262 (9th Cir. 1992)(issuing judge was out of town for several days after the tapes were ready for sealing); U.S. v. Rodriquez, 786 F.2d 472 (2d Cir. 1986)(absence of issuing judge is no longer an acceptable explanation for delay because circuit precedent has established that the tapes can be sealed by a judge other than the issuing judge); United States v. Fury, 554 F.2d 522 (2d Cir.)(six-day delay because issuing judge was on vacation and unavailable), cert. denied, 433 U.S. 910 (1977); United States v. Blanco, 1994 WL 695396 (N.D. Cal. December 8, 1994) (unreported) (tapes were ready for sealing within three days of termination, but due to continuing unavailability of the issuing judge and other district judges, a magistrate granted the government's request for a sealing order sixteen days after termination of the interception, and upon return to the district, the issuing judge granted the government's application for an order ratifying the magistrate's sealing order).

The failure to seal immediately because of unexpected resource or personnel shortages has been deemed a "satisfactory explanation." Pedroni, supra (agent in charge of case took time to interview two potential witnesses who became available at the time when the tapes were being prepared for sealing); United States v. Rodriquez, 786 F.2d 472 (2d Cir. 1986)(fourteen-day

delay because supervising attorney occupied with another trial); United States v. Massino, 784 F.2d 153 (2d Cir. 1986)(fifteen-day delay because government diverted personnel to investigate leak threatening investigation); United States v. Scafidi, 564 F.2d 633 (2d Cir. 1977)(seven-day delay because prosecutor preoccupied with upcoming trial). Compare United States v. Quintero, 38 F.3d 1317 (3d Cir. 1994)(because the AUSA's caseload was foreseeable, the tapes should have been sealed immediately), cert. denied, 513 U.S. 1195 (1995).

A government attorney's objectively reasonable "mistake of law" may be a satisfactory explanation for a sealing delay. United States v. Wilkinson, 53 F.3d 757 (6th Cir. 1995)("good faith" misunderstanding of court order); United States v. Vastola, 25 F.3d 164 (3d Cir.)(affirmed district court's finding on remand that AUSA's combined reading of the law and her reliance on the opinions of more experienced colleagues on the sealing issue was minimally sufficient to meet the standards of a reasonably prudent attorney), cert. denied, 513 U.S. 1015 (1994); United States v. Carson, 969 F.2d 1480 (3d Cir. 1992)(even if a government attorney's legal conclusion was found to be unreasonable, the explanation for the delay would still be an objectively reasonable "mistake of law" if the government could show that its attorney had adequately researched the law or had otherwise acted reasonably). Notwithstanding the overall favorable case law, the ESU still stresses the importance of sealing every thirty days to obviate the issue at trial and on appeal.

4. How to Seal/Custody of the Tapes

Sealing is accomplished by making the original recordings of the intercepted conversations available to the judge who issued the interception order. The statutory sealing requirements are met when the government attorney advises the district judge that the tapes are available for inspection at the time he presents motions for orders sealing them; it is not necessary that the recordings be sealed in the judge's presence. See United States v. Abraham, 541 F.2d 624 (6th Cir. 1976); United States v. Kincaide, 145 F.3d 771 (6th Cir. 1998). Typically, however, the AUSA and the case agent will deliver the tapes to the judge, who will then physically seal the box containing the tapes, initialling and dating the evidence tape. The judge will then issue a sealing order and determine where the tapes are to be kept. The judge will usually order that the investigative agency retain custody of the sealed tape recordings.

5. Suppression for Failure to Seal Properly

Failure to seal the tapes properly or to offer a satisfactory explanation for a sealing delay will likely result in suppression of the evidence. Compare United States v. Carson, 969 F.2d 1480 (3d Cir. 1992)(thirty-four-day delay in sealing for purpose of audio enhancement was not a satisfactory explanation; government should have sealed the tapes and sought order to unseal for purpose of enhancement) with United States v. Fiumara, 727 F.2d 209 (2d Cir.)(unsealing order authorized the government to unseal the tapes to the limited extent necessary to duplicate, disclose, and otherwise make use of them; a private audio expert's "custody of the tapes for purposes of enhancement and duplication" was consistent with this order), cert. denied, 466 U.S. 951 (1984). See also United States v. Feiste, 961 F.2d 1349 (8th Cir. 1992)(suppression ordered because 31 day sealing delay was "simply matter of convenience").

6. Resealing

Once the trial has ended and the need for the electronic surveillance tapes has concluded, the original tapes should be resealed in order to preserve their integrity for use in other proceedings. Even after surveillance tapes have been used in one judicial proceeding, they may not be admitted into evidence in another without a judicial seal "or a satisfactory explanation for the absence thereof." 18 U.S.C. § 2518(8)(a). See United States v. Boyd, 208 F.3d 638 (7th Cir. 2000); United States v. Long, 917 F.2d 691 (2d Cir. 1990); United States v. Scopo, 861 F.2d 339 (2d Cir. 1988), cert. denied, 490 U.S. 1022 (1989).

X. INVENTORY NOTICE

Title 18, United States Code, Section 2518(8)(d) requires an inventory notice to be served on persons named in the order, and "...other such parties to intercepted communications as the judge may determine ... is in the interest of justice ..." within a reasonable time, but not later than 90 days after the end of the last extension order. The government has an obligation to categorize those persons whose communications were intercepted so that the judge may make a reasoned determination about whether they will receive inventory notice. United States v. Donovan, 429 U.S. 413 (1977); United States v. Alfonso, 552 F.2d 605 (5th Cir. 1977), cert. denied, 434 U.S. 857 (1977); United States v. Chun, 503 F.2d 533 (9th Cir. 1974). The inventory should state that an order or application was entered, the date it was entered and the period of authorized interceptions, or the denial of interception, as well as whether communications were intercepted. Upon a showing of good cause (e.g., impairment of an ongoing investigation), the court may delay service of inventory notice.

Absent a showing of bad faith or actual prejudice, the failure to serve a formal inventory notice under section 2518(8)(d) does not justify suppression. Donovan, supra; United States v. DeJesus, 887 F.2d 114 (6th Cir. 1989); United States v. Davis, 882 F.2d 1334 (8th Cir. 1989), cert. denied, 494 U.S. 1027 (1990); United States v. Savaiano, 843 F.2d 1280 (10th Cir. 1988). Suppression will likely occur only when the statutory violation arose from a conscious decision by the federal authorities to violate the law and to prevent an individual or group of individuals from receiving the post-interception notice. United States v. Harrigan, 557 F.2d 879 (1st Cir. 1977).

XI. DISCLOSURE OF TITLE III EVIDENCE

1. 18 U.S.C. § 2517(1), (2), (6), (7), (8) - Use and Disclosure of Interception Information

Briefly, section 2517(1) authorizes an investigative or law enforcement officer to disclose, without prior court approval, the contents of intercepted communications to another law enforcement or investigative officer, as defined by 18 U.S.C. § 2510(7), to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the information.

Section 2517(2) permits an investigative or law enforcement officer, without prior court approval, to use the contents of properly obtained electronic surveillance evidence to the extent that such use is appropriate to the proper performance of his official duties. See Apampa v. Layng, 157 F.3d 1103 (7th Cir. 1998)(disclosure of wiretap information in public indictment is proper use under 2517(2)); United States v. Gerena, 869 F.2d 82 (2d Cir. 1989)(use in search warrants); United States v. O'Connell, 841 F.2d 1408 (8th Cir.)(disclosure to secretaries and intelligence analysts), cert. denied, 487 U.S. 1210 (1988); United States v. Ricco, 566 F.2d 433 (2d Cir. 1977)(to refresh recollection of a witness), cert. denied, 436 U.S. 926 (1978); United States v. Rabstein, 554 F.2d 190 (5th Cir. 1977)(for voice identification).

Section 2517(6) permits any investigative or law enforcement officer, or attorney for the Government to disclose interception information to other Federal law enforcement, intelligence, protective, immigration, national defense, or national security officials to the extent the information includes foreign intelligence or counterintelligence, to assist the receiving official in the performance of his official duties.

Section 2517(7) permits any investigative or law enforcement officer, or other Federal official in carrying out official

duties as such Federal official, to disclose the contents of intercepted communications and evidence derived therefrom to "foreign investigative or law enforcement officers" to the extent such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure. In addition, Section 2517(7) authorizes foreign investigative or law enforcement officers to use or disclose such contents or derivative evidence to the extent appropriate to the performance of their official duties.

Section 2517(8) permits any investigative or law enforcement officer, or other Federal official in carrying out official duties as such Federal official, to disclose the contents of intercepted communications and evidence derived therefrom to any appropriate Federal, State, local, or "foreign government official" to the extent the contents or derivative evidence reveals a threat of actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power, sabotage, terrorism, or clandestine intelligence gathering activities by an intelligence service or network of a foreign power or by an agent of a foreign power, within the United States or elsewhere, for the purpose of preventing or responding to such threat. The foreign official who receives such information may use it only consistent with such guidelines as the Attorney General and Director of Central Intelligence shall jointly issue.

While it is clear from the legislative history and the case law cited above that section 2517 allows the disclosure of Title III information for any legitimate investigative purpose associated with the development of a criminal case, the release of the information under this section for other purposes is the subject of dispute. It has been argued successfully that section 2517 also permits disclosure for use in various civil matters, such as forfeiture cases, congressional hearings or investigations, state bar disciplinary proceedings, and civil tax investigations. See Berg v. Michigan Attorney Grievance Commission, 49 F.3d 1188 (6th Cir. 1995)("once conversations are lawfully intercepted, disclosure is not limited to criminal proceedings"; upholding disclosure of Title III evidence to attorney grievance commission); In re Grand Jury Proceedings, 841 F.2d 1048 (11th Cir. 1988)(House committee investigating whether impeachment proceedings are warranted falls within the definition of "investigative officer"); United States v. All Right, Title and Interest..., 830 F. Supp. 750 (S.D.N.Y. 1993)(AUSAs, whether working on criminal or civil matters, fall within section 2510(7)'s definition of an "investigative or law enforcement officer").

In any event, when in doubt about whether the disclosure or use of electronic surveillance evidence is permitted, obtain a

court order pursuant to 18 U.S.C. § 2518(8)(b) authorizing the disclosure and use for "good cause." (Although section 2518(8)(b) provides for the disclosure of Title III "applications and orders," the legislative history reflects that it was also intended to apply to the disclosure of the Title III recordings themselves, as well as any related documentation. See also In re Grand Jury Proceedings, 841 F.2d 1048, 1053 n.9 (11th Cir. 1988). Thus, the Department has successfully obtained disclosure orders under section 2518(8)(b) for the release of the tapes of intercepted conversations.) The Department recommends this course of action because 18 U.S.C. § 2520 provides that a good faith reliance on a court order is a complete defense to civil and criminal actions for unauthorized disclosure of electronic surveillance information. A sample disclosure application and order can be found in the "FORMS" section of this manual.

When disclosing and using electronic surveillance information, the government must ensure that the disclosure of the electronic surveillance information does not abridge the privacy rights of parties not charged with any crime, or jeopardize an ongoing criminal investigation. See United States v. Dorfman, 690 F.2d 1230 (7th Cir. 1982)(disclosure to a limited audience of "professionally interested strangers" in the context of their official duties is not the equivalent to disclosure to the public; "Title III does not allow public disclosure of all lawfully obtained wiretap evidence just because a few officers are privy to its contents"). See also Certain Interested Individuals v. Pulitzer Pub., 895 F.2d 460 (8th Cir.)(pre-indictment stage of criminal case "tips the balance ... in favor of the privacy interests and against disclosure of even redacted version of the search warrant affidavits at this time"), cert. denied, 498 U.S. 880 (1990); United States v. Shenberg, 791 F. Supp. 292 (S.D. Fla. 1991)(court denied media's motion seeking access to search warrants containing Title III interceptions until their admissibility was established); State v. Gilmore, 549 N.W.2d 401 (Wis. 1996)(Wisconsin electronic surveillance disclosure provisions, which are virtually identical to 18 U.S.C. § 2517(1), (2), bar the state from including legally intercepted communications in a criminal complaint unless the complaint is filed under seal). In this regard, the United States Attorney's Manual, at 9-7.250, recommends placing under seal Title III-related material and seeking a protective order under Fed. R. Crim. Proc. 16, asking the court to forbid defense counsel from publicly disclosing the information.

2. 18 U.S.C. § 2517(3) - Testimonial Use

Section 2517(3) allows a person, without prior court approval, to disclose electronic surveillance information, or any derivative evidence, while giving testimony under oath in any

federal, state, or local proceeding. It should be noted that the prerequisite for the testimonial use of electronic surveillance evidence is the "presence of the seal ... or a satisfactory explanation for the absence thereof...." 18 U.S.C. § 2518(8)(a). See Certain Interested Individuals v. Pulitzer Pub., 895 F.2d 460 (8th Cir. 1990)(disclosure of wiretap information in a search warrant affidavit is not the testimonial disclosure contemplated in section 2517(3), even though affidavits are prepared under oath or affirmation), cert denied, 498 U.S. 880 (1990).

3. 18 U.S.C. § 2517(4) - Privileged Communications

This section merely provides: "No other privileged wire, oral, or electronic communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character."

4. 18 U.S.C. § 2517(5) - Use of "Other Crimes" Evidence

Section 2517(5) pertains to the interception of conversations that relate to offenses other than those specified in the authorization order. In pertinent part, that section states: "When ... a law enforcement officer ... intercepts wire, oral, or electronic communications relating to offenses other than those specified in the order ..., the contents thereof, and evidence derived therefrom, may be disclosed or used [for law enforcement purposes] ..." or disclosed under oath in any proceeding when the "... judge finds on subsequent application that the contents were otherwise intercepted in accordance with [Title III]." A sample 2517(5) application and order can be found in the "FORMS" section of this manual.

If, for example, the Title III order authorizes the interception of communications related to narcotics offenses, and during the course of the interception period, conversations concerning loansharking are overheard, section 2517(5) allows the continued interception of those conversations and their use for law enforcement purposes. The court should, however, be notified as soon as practicable that conversations about other offenses are being monitored, and the new offenses should be added to the pleadings if an extension order is obtained. By including the new offenses in the extension order, the government may use that evidence in future proceedings without having to obtain additional court-authorization later. If no extension order is obtained and the government wishes to use that evidence in a future proceeding, an order should be obtained as soon as practicable pursuant to 18 U.S.C. § 2517(5). See United States v. Barnes, 47 F.3d 963 (8th Cir. 1995)(2517(5) order may be obtained after the "other offense" evidence is presented to the grand jury); United States v. Brodson, 528 F.2d 214 (7th Cir.

1975)(2517(5) order must be obtained before "other offense" evidence is submitted to the grand jury); United States v. Vario, 943 F.2d 236 (2d Cir. 1991)(four-year total delay, seven months between when law enforcement realized relevance of tapes to instant case and when the order was obtained), cert. denied, 502 U.S. 1036 (1992); United States v. Van Horn, 789 F.2d 1492 (11th Cir.)(the government's request under section 2517(5) for testimonial use of state wiretap evidence in a federal drug prosecution was timely, although it was made 22 months after federal agents learned of the state wiretap and five months after they learned of the contents of the state wiretap), cert. denied, 479 U.S. 854 (1986); United States v. Arnold, 773 F.2d 823 (7th Cir. 1985)(thirty-one-month delay in seeking order); United States v. Southard, 700 F.2d 1 (1st Cir. 1983)(nineteen-month delay between recording of conversations and application for their use).

The purpose of section 2517(5) is to ensure that the interception of the other offenses was truly incidental to the interception of offenses for which the government had court-authorization. As mentioned previously, with regard to interceptions involving wire and oral communications, the government may only use electronic surveillance to investigate certain crimes and only those crimes; the government cannot allege that it will intercept communications about predicate offenses (those listed under section 2516(1)) and in actuality intercept communications about offenses which are not predicates under Title III or Title III predicates for which they did not have probable cause. See United States v. London, 66 F.3d 1227 (1st Cir. 1995)("the interception is unlawful only when it is motivated by an illicit purpose - e.g., 'subterfuge' interceptions where the government applies to intercept conversations relating to offenses specified in 18 U.S.C. § 2516(1) while intending to intercept conversations relating to offenses for which interceptions are unauthorized or which it has no probable cause to obtain an interception order"), cert. denied, 116 S. Ct. 1542 (1996); United States v. Homick, 964 F.2d 899 (9th Cir. 1992); United States v. Ardito, 782 F.2d 358 (2d Cir.), cert. denied, 475 U.S. 1141 (1986); United States v. Van Horn, 789 F.2d 1492 (11th Cir.), cert. denied, 479 U.S. 854 (1986).

"Other" offenses under section 2517(5) may include offenses, federal as well as state, not listed in 18 U.S.C. § 2516, as well as additional predicate offenses not set out in the court order, as long as there is no indication of bad faith or subterfuge on the part of the government. See In re Grand Jury Subpoena Served on Doe, 889 F.2d 384 (2d Cir. 1989)(tax offenses); United States v. Shnayderman, 1993 WL 524782 (E.D. Pa. Dec. 17, 1993) (unreported)(tax offenses).

XII. DISCOVERY

1. 18 U.S.C. § 2518(9), 2518(10)(a)

Section 2518(9) requires the government to furnish a defendant with a copy of the court order and accompanying application under which the interception was authorized or approved, ten days before the contents of any wire, oral, or electronic communication is received in evidence in any trial, hearing, or other proceeding in a federal or state court, unless the court waives the ten-day period upon a showing by the government that compliance is not possible and that the defendant will not be prejudiced. See In re Grand Jury Proceedings, 841 F.2d 1048, 1053 n.9 (11th Cir. 1988)(construing "applications" and "orders" to include related documentation and intercepted conversations).

While section 2518(9) requires the government to disclose wiretap applications and orders to a defendant, the "good cause" requirement of section 2518(8)(b) and the "interest of justice" standard in section 2518(10)(a) make it clear that the defendant is entitled only to that information that is relevant to his defense and is not protected from disclosure by some other constitutional right or privilege. See United States v. Orena, 883 F. Supp. 849 (E.D.N.Y. 1995)("[t]here is no statutory requirement that all recordings made pursuant to the court order be produced. To the contrary, section 2518(10)(a) specifically provides that it rests within the discretion of the trial court to decide whether intercepted communications should be furnished to a defendant"); United States v. Yoshimura, 831 F. Supp. 799 (D. Hawaii 1993); Application of U.S. for an Order Authorizing Interception of Wire and Oral Communications, 495 F. Supp. 282 (E.D. La. 1980); United States v. Ferle, 563 F. Supp. 252 (D.R.I. 1983).

2. The Federal Rules

The discovery of electronic surveillance evidence must be made in accord not only with the wiretap statutes, but also with the Federal Rules of Criminal Procedure. For examples, see United States v. Howell, 514 F.2d 710 (5th Cir. 1975), cert. denied, 429 U.S. 838 (1976); United States v. Feola, 651 F. Supp. 1068 (S.D.N.Y. 1987), aff'd, 875 F.2d 857 (1989).

While electronic surveillance evidence and its related documentation are discoverable, work product exposing the government's theory is not. Feola, supra; United States v. Payden, 613 F. Supp. 800 (S.D.N.Y. 1985)(the court denied requests for analysis performed on toll records and other conclusions of investigative officers; these were internal

government documents made in connection with the investigation of the case). See also United States v. Wright, 121 F. Supp.2d 1344 (D. Kan. 2000) (agent's summary of call or conversation is protected work product); United States v. Nakashian, 635 F. Supp. 761 (S.D.N.Y. 1986), cert. denied, 484 U.S. 963 (1987).

XIII. PEN REGISTERS/TRAPS AND TRACES

Except as provided in 18 U.S.C. § 3121, no person may install or use a pen register or a trap and trace device without first obtaining a court order under 18 U.S.C. § 3123 or under the Foreign Intelligence Surveillance Act (50 U.S.C. 1801, et seq.). The application may be made by an attorney for the government or a state law enforcement or investigative officer, and must certify that the information likely to be obtained is relevant to an ongoing criminal investigation. Unlike Title III pleadings, a pen register application need not establish probable cause and does not require prior Department approval. The order, which is valid for sixty days (and may be extended for additional sixty-day periods), must specify the identity, if known, of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied; the identity, if known, of the person who is the subject of the criminal investigation; the attributes of the communications to which the order applies, including the number or other identifier and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied, and, in the case of an order authorizing installation and use of a trap and trace device under subsection 3123(a)(2)(State court order), the geographic limits of the order; the offense(s) to which the information to be obtained from the pen register or trap and trace will relate; and direct, upon the request of the applicant, the furnishing of information, facilities, and technical assistance necessary to accomplish the installation of the pen register or trap and trace device. The order should also direct that the application and order be sealed until otherwise ordered by the court, and that no disclosure of the existence of the pen register or trap and trace or the existence of the investigation be made to the subscriber or other persons until directed by the court. See generally Fregoso, supra ("The judicial role in approving use of trap and trace devices is ministerial in nature"); In re Application of United States for Order Authorizing Installation and Use of Pen Register and Trap and Trace Device, 846 F. Supp. 1555 (M.D. Fla. 1994)(the court must issue a pen register order on mere statutory certification by the government). A pen register/trap and trace order is executable anywhere within the United States and, upon service, the order applies to any person or entity providing wire or electronic communication service in the United States whose

assistance may facilitate the execution of the order. Whenever such an order is served on any person or entity not specifically named in the order, upon request of such person or entity, the attorney for the Government or law enforcement or investigative officer that is serving the order shall provide written or electronic certification that the order applies to the person or entity being served. 18 U.S.C. § 3123(a).

Section 3121(c) requires that a government agency authorized to install and use a pen register or trap and trace device use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing, routing, addressing, and signaling information utilized in the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications.

Section 3127(3) defines a "pen register" as "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business."

Section 3127(4) defines a "trap and trace device" as "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication."

Pen register and trap and trace devices may obtain any non-content information - all "dialing, routing, addressing, and signaling information" - utilized in the processing and transmitting of wire and electronic communications. Such information includes IP addresses and port numbers, as well as the "To" and "From" information contained in an e-mail header. Pen/trap orders cannot, however, authorize the interception of the content of a communication, such as words in the "subject line" or the body of an e-mail. Agents and prosecutors with questions about whether a particular type of information constitutes content should contact the Office of Enforcement Operations in the telephone context (202-514-6809) or the

Computer Crime and Intellectual Property Section in the computer context (202-514-1026).

On May 24, 2002, The Deputy Attorney General issued a Memorandum setting forth the Justice Department's policy regarding avoidance of "overcollection" in the use of pen registers and trap and trace devices deployed under 18 U.S.C. § 3121, *et seq.*. This policy prohibits the affirmative investigative use of any "content" collected despite the use of reasonably available technology, except to prevent an immediate danger of death, serious physical injury, or harm to the national security. This policy memorandum may be found on USABook Online at the following URL: http://10.173.2.12/usao/eousa/ole/tables/misc/penreq.pdf . On June 3, 2002, this memorandum was distributed by electronic mail to all United States Attorneys, First Assistant United States Attorneys and Criminal Chiefs.

The "FORMS" section of this manual contains a combined 3123/2703 application and order that addresses the treatment of "post-cut-through digits" captured during pen/trap operations.

XIV. CELL SITE SIMULATORS/DIGITAL ANALYZERS/TRIGGERFISH

A cell site simulator, digital analyzer, or a triggerfish can electronically force a cellular telephone to register its mobile identification number ("MIN," i.e., telephone number) and electronic serial number ("ESN," i.e., the number assigned by the manufacturer of the cellular telephone and programmed into the telephone) when the cellular telephone is turned on. Cell site data (the MIN, the ESN, and the channel and cell site codes identifying the cell location and geographical sub-sector from which the telephone is transmitting) are being transmitted continuously as a necessary aspect of cellular telephone call direction and processing. The necessary signaling data (ESN/MIN, channel/cell site codes) are not dialed or otherwise controlled by the cellular telephone user. Rather, the transmission of the cellular telephone's ESN/MIN to the nearest cell site occurs automatically when the cellular telephone is turned on. This automatic registration with the nearest cell site is the means by which the cellular service provider connects with and identifies the account, knows where to send calls, and reports constantly to the customer's telephone a read-out regarding the signal power, status and mode.

If the cellular telephone is used to make or receive a call, the screen of the digital analyzer/cell site simulator/ triggerfish would include the cellular telephone number (MIN), the call's incoming or outgoing status, the telephone number dialed, the cellular telephone's ESN, the date, time, and

duration of the call, and the cell site number/sector (location of the cellular telephone when the call was connected).

Digital analyzers/cell site simulators/triggerfish and similar devices may be capable of intercepting the contents of communications and, therefore, such devices must be configured to disable the interception function, unless interceptions have been authorized by a Title III order.

Because section 3127 of Title 18 defines pen registers and trap and trace devices in terms of recording, decoding or capturing dialing, routing, addressing, or signaling information, a pen register/trap and trace order must be obtained by the government before it can use its own device to capture the ESN or MIN of a cellular telephone, even though there will be no involvement by the service provider. See discussion below in Chapter XV.

XV. THE LEGAL AUTHORITIES REQUIRED TO LOCATE CELLULAR TELEPHONES

WARNING: THIS ISSUE HAS BEEN THE SUBJECT OF EXTENSIVE LITIGATION RECENTLY. THE INFORMATION CONTAINED IN THIS ARTICLE IS NO LONGER CURRENT. IF YOU HAVE QUESTIONS OR CONCERNS, PLEASE CONTACT THE COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION AT 202.514.1026.

[The following analysis was prepared by attorney Richard W. Downing of the Computer Crime and Intellectual Property Section, Criminal Division, U.S. Department of Justice]

I. Compelling Providers to Disclose Cell-phone Location Records

In order to provide service to cellular telephones, providers have the technical capability to collect information such as the cell tower nearest to a particular cell phone, the portion of that tower facing the phone, and often the signal strength of the phone. Depending on the number of towers in a particular area and other factors, this information may be used to identify the location of a phone to within a few hundred yards. Some providers routinely update this information at all times that the cell phone is turned on; others update it only when the user places a call. Carriers generally keep detailed historical records of this information for billing and other business purposes. At times, law enforcement authorities seek to compel carriers to preserve that information prospectively for use in a criminal investigation.

A. Obtaining Historical Records from Cellular Providers

Law enforcement investigators may use a search warrant or an order under section 2703(d) of title 18 in order to obtain historical records from cellular carriers. Section 2703(c)(1) provides:

> A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity
>
> > (A) obtains a warrant issued using the procedures described in the Federal Rules of criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant;
> >
> > (B) obtains a court order for such disclosure under subsection (d) of this section;
> >
> > ....

18 U.S.C. 2703(c)(1).

It remains doubtful whether law enforcement authorities may use a subpoena to obtain this same information. The amendments to section 2703© enacted in the USA PATRIOT Act of 2001 (the "USA PATRIOT Act") broadened the scope of records that may be obtained using a subpoena. In section 2703©, the Act changed "local and long distance telephone toll billing records" to "local and long distance telephone *connection* records, *or records of session times and durations*." The legislative history does not comment on the intent of this change nor did this topic arise in any of the negotiations surrounding the passage of the Act. There is no evidence, however, that Congress expanded the scope of this definition in order to include cell phone location information. Thus, although there are arguments on both sides, the better practice is to use 2703(d) orders and search warrants - rather than subpoenas - to obtain cell phone location information from providers.

B. Compelling Providers to Collect Cell Phone Location Information Prospectively

In order to require a provider to collect cell-phone location information prospectively (e.g., for the following 60 days), law enforcement authorities must obtain a court order. One possibility is an order under section 3123, the Pen Register and Trap and Trace Statute ("Pen/Trap Statute"). The USA PATRIOT Act amended the definitions of "pen register" and "trap and trace device" to include any device or process that collects the "dialing, routing, addressing, and signaling information" associated with a communication. Although no legislative history directly addresses whether "signaling" includes such information as the nearest cell tower, the face used by that cell tower, and the signal strength, a House Judiciary Committee Report on a preceding bill (commenting on language identical to that eventually enacted in the USA PATRIOT Act) suggests that the pen/trap statute governs such information. It states:

> This concept, that the information properly obtained by using a pen register or trap and trace device is non-content information, *applies across the board to all communications media*.

H.R. Rept. 107-236, 107th Cong., 1st Sess. 53 (2001) (Rept. to Accompany H.R. 2975) ("House Report") (emphasis supplied). For a more in-depth discussion of this idea, see *infra* Section II.B.

Even if the pen/trap statute's amended definitions include such information, however, it remains doubtful that this non-specific language overrules the previously existing prohibition on carriers providing location information in response to a pen/trap order. In 1994, Congress explicitly prohibited providers from providing cell phone location information in response to a pen/trap order:

> (a) ... a telecommunications carrier shall ensure that its equipment, facility or services that provide a customer or subscriber with the ability to originate, terminate, or direct communications are capable of -
>
> ...
>
> (2) expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to access call-identifying information that is reasonably available to the carrier-
>
> ...
>
> *except that, with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices (as defined in section 3127 of title 18, United States Code), such call-identifying information shall not include any information that may disclose the physical location of the subscriber* (except to the extent that the location may be determined from the telephone number)....

Public Law 103-414, sec. 103(a) (1994) ("CALEA") (emphasis supplied). A court is likely to find that this clear expression of Congressional intent, which makes explicit reference to the definitions of pen registers and trap and trace devices, continues to prohibit providers from supplying cell phone location information in response to a pen/trap order.

Because of the 1994 prohibition, law enforcement authorities have sought other means to compel providers to supply this information prospectively. Most commonly, investigators have used orders under section 2703(d) to obtain this information. Although section 2703(d) generally applies only to stored communications, nothing in that section requires that the provider possess the records at the time the order is executed. Moreover, use of such an order does not improperly evade the intent of the CALEA prohibition. Section 2703(d) court orders provide greater privacy protection and accountability than pen/trap orders by requiring (1) a greater factual showing by law enforcement and (2) an independent review of the facts by a court. Indeed, the very language of the CALEA prohibition - limiting its application "to information acquired *solely* pursuant to the authority for pen registers and trap and trace devices" - indicates that Congress intended that the government be able to obtain this information using some other legal process. Public Law 103-414, sec. 103(a) (emphasis supplied). Thus, 2703(d) orders are an appropriate tool to compel a provider to collect cell phone location information prospectively.

Finally, some have suggested that such orders should rely on the Mobile Tracking Devices statute, 18 U.S.C. § 3117. Although making reference to this statute would not be harmful, it does not provide much legal support for such an order. The statute refers to the "installation" of a "mobile tracking device." This language probably would apply to the provider's use of a software program to track the location of a particular cell phone, even though such a program is not literally a physical "device."

More importantly, however, the language of section 3117 assumes that the court has authority from some other source to order the installation of the device. Section 3117 only gives the court authority to authorize the use of such a device outside of the court's jurisdiction. This added benefit will rarely be an issue where a court issues a 2703(d) order for the collection of cell phone location information by a provider, since amendments in the USA PATRIOT Act assure that 2703(d) orders have nationwide effect. Moreover, a provider may well be able to execute such an order at one central point and not require the "use" of the device outside of the court's jurisdiction.

II. Collection of Cell Phone Location Information Directly by Law Enforcement

Law enforcement possesses electronic devices that allow agents to determine the location of certain cellular phones by the electronic signals that they broadcast. This equipment includes an antenna, an electronic device that processes the signals transmitted on cell phone frequencies, and a laptop computer that analyzes the signals and allows the agent to configure the collection of information. Working together, these devices allow the agent to identify the direction (on a 360 degree display) and signal strength of a particular cellular phone while the user is making a call. By shifting the location of the device, the operator can determine the phone's location more precisely using triangulation.

In order to use such a device the investigator generally must know the target phone's telephone number (also known as a Mobile Identification Number or MIN). After the operator enters this information into the tracking device, it scans the surrounding airwaves. When the user of that phone places or receives a call, the phone transmits its unique identifying information to the provider's local cell tower. The provider's system then automatically assigns the phone a particular frequency and transmits other information that will allow the phone properly to transmit the user's voice to the cell tower. By gathering this information, the tracking device determines which call (out of the potentially thousands of nearby users) on which to home in. While the user remains on the phone, the tracking device can then register the direction and signal strength (and therefore the approximate distance) of the target phone.

A. Use of Law Enforcement Cell Phone Tracking Devices Prior to the USA PATRIOT Act of 2001

In 1994, the Office of Enforcement Operations opined that investigators did not need to obtain any legal process in order to use cell phone tracking devices so long as they did not capture the numbers dialed or other information "traditionally" collected using a pen/trap device. This analysis concluded that the "signaling information" automatically transmitted between a cell phone and the provider's tower does not implicate either the Fourth Amendment or the wiretap statute because it does not constitute the "contents" of a communication. Moreover, the analysis reasoned - prior to the 2001 amendments - that the pen/trap statute did not apply to the collection of such information because of the narrow definitions of "pen register" and "trap and trace device." Therefore, the guidance concluded, since neither the constitution nor any statute regulated their use, such devices did not require any legal authorization to operate.

B. The Pen/Trap Statute, As Amended By The USA PATRIOT Act of 2001

Although the analysis remains unchanged with respect to the Fourth Amendment and the wiretap statute, substantial amendments to the definitions of "pen register" and "trap and trace device" in the USA PATRIOT Act alter the applicability of the pen/trap statute. The new definitions, on their face, strongly suggest that the statute now governs the use of such devices. Where the old definition of "pen register" applied only to "numbers dialed or otherwise transmitted," "pen register" now means

> a device or process which records or decodes dialing, routing, addressing, and signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted....

18 U.S.C. § 3127(3). "Signaling information" is a broader term that encompasses other kinds of non-content information used by a communication system to process communications. This definition appears to encompass all of the non-content information passed between a cell phone and the provider's tower.

Similarly, the USA PATRIOT Act broadened the definition of "trap and trace device." Where before the definition included only "the originating number of an instrument or device," the new definition covers "the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication...." 18 U.S.C. § 3127(4). Like the definition of "pen register," this broader definition appears to include such information as the

transmission of a MIN, which identifies the source of a communication.

Moreover, the scant legislative history that accompanied passage of the Act suggests Congress intended that the new definitions apply to all communications media, instead of focusing solely on traditional telephone calls. Although the House Report cannot definitively state the intent of both houses of Congress when passing the final bill, it does strongly suggest that Congress intended that the statute would apply to all technologies:

> This section updates the language of the statute to clarify that the pen/register [sic] authority applies to modern communication technologies. Current statutory references to the target "line," for example, are revised to encompass a "line or other facility." Such a facility includes: *a cellular telephone number; a specific cellular telephone identified by its electronic serial number (ESN);* an Internet user account or e-mail address; or an Internet Protocol (IP) address, port number, or similar computer network address or range of addresses. In addition, because the statute takes into account a wide variety of such facilities, section 3123(b)(1)© allows applicants for pen register or trap and trace orders to submit a description of the communications to be traced using any of these or other identifiers.
>
> Moreover, the section clarifies that orders for the installation of pen register and trap and trace devices may obtain *any* non-content information - "dialing, routing, addressing, and signaling information" - utilized in the processing and transmitting of wire or electronic communications....
>
> This concept, that the information properly obtained by using a pen register or trap and trace device is non-content information, *applies across the board to all communications media* ... ([and includes] packets that merely request a telnet connection in the Internet context).

H.R. Rept 107-236, at 52-53 (emphasis added). Indeed, this last reference to a packet requesting a telnet session - a piece of information passing between machines in order to establish a communication session for the human user - provides a close analogy to the information passing between a cell phone and the nearest tower in the initial stages of a cell phone call.

Finally, the House Report recognizes that pen registers and trap and trace devices could include devices that collect information remotely. The Report states:

> Further, *because the pen register or trap and trace 'device' is often incapable of being physically 'attached' to the target facility due to the nature of modern communication technology*, section 101 makes two other related changes. First, in recognition of the fact that such functions are commonly performed today by software instead of physical mechanisms, the section allows the pen register or trap and trace device to be 'attached or applied' to the target facility [such as an ESN]. Likewise, the definitions of 'pen register' and 'trap and trace device' in section 3127 are revised to include an intangible 'process' (such as a software routine) which collects the same information as a physical device.

H.R. Rept 107-236, at 53 (emphasis added). Thus, the statutory text and legislative history strongly suggest that the pen/trap statute governs the collection of cell phone location information directly by law enforcement authorities.

C. The Inapplicability of CALEA's Prohibition on Collection Using Pen/Trap Authority

In passing CALEA in 1994, Congress required providers to isolate and provide to the government certain information relating to telephone communications. At the same time that it created these obligations, it created an exception: carriers shall not provide law enforcement with "any information that may disclose the physical location of the subscriber" in response to a pen/trap order. (A fuller quotation of the language appears, above, in Section I.B.). By its very terms, this prohibition applies only to information collected by a provider and not to information collected directly by law enforcement authorities. Thus, CALEA does not bar the use of pen/trap orders to authorize the use of cell phone tracking devices used to locate targeted cell phones.

D. Conclusion

The amended text of the pen/trap statute and the limited legislative history accompanying the 2001 amendments strongly suggest that the non-content information that passes between a cellular phone and the provider's tower falls into the definition of "dialing, routing, addressing, and signaling information" for purposes of the definitions of "pen register" and "trap and trace device." A pen/trap authorization is therefore the safest method of allowing law enforcement to collect such transmissions directly using its own devices.

XVI. MOBILE TRACKING DEVICES

Tracking devices ("bumper beepers") are not regulated by Title III, and their use is governed by existing case law. The seminal cases in this area are United States v. Knotts, 460 U.S. 276 (1983)(Fourth Amendment not implicated) and United States v. Karo, 468 U.S. 705 (1984)(warrantless monitoring in an area invoking a reasonable expectation of privacy may violate Fourth Amendment), which set forth the Fourth Amendment standards governing the use of beepers. Basically, a search warrant is needed only when the object to which the beeper is attached enters an area that carries a legitimate expectation of privacy, such as the inside of a vehicle or a private residence. Since it often cannot be determined in advance whether a package containing a beeper will be taken inside a place where a person has a valid expectation of privacy, a search warrant should be obtained to cover that eventuality. But see U.S. v. Forest, 355 F.3d 942 (6th Cir. 2004) (permitting warrantless capture of cell-site data); U.S. v. McIver, 186 F.3d 1119 (9th Cir. 1999) (permitting warrantless use of GPS device and Birddog beeper); United States v. Jones, 31 F.3d 1304 (4th Cir. 1994)(Postal Inspectors' use of beeper to monitor movement of a stolen mail pouch in defendant's vehicle did not constitute a search).

ECPA did, however, change the existing jurisdictional requirement relating to tracking devices. 18 U.S.C. § 3117 provides that a court order issued for such a device is valid anywhere within the United States. This obviates the need to obtain a new order whenever the object containing the device crosses state or district lines. United States v. Gbemisola, 225 F.3d 753 (D.C. Cir. 2000)(contains an explanation of 18 U.S.C. § 3117).

XVII. VIDEO SURVEILLANCE

Video surveillance, or the use of closed circuit television (CCTV), is not regulated by Title III, but is frequently part of an application for electronic surveillance. When there is a reasonable expectation of privacy in the place to be videotaped, prior approval from an appropriate DOJ official and a court order are required before such video surveillance may be used in an investigation. Briefly, a court order and prior Department approval are required unless the surveillance is used to record events in public places or places where the public has unrestricted access, and where the camera equipment can be installed in places to which investigators have lawful access. See generally Thompson v. Johnson County Community College, 930 F. Supp. 501 (D. Kan. 1996)(college's warrantless use of CCTV to monitor locker area of storage room for thefts and weapons was constitutional).

If a court order is required, the pleadings are to be based on Rule 41(b) of the Federal Rules of Criminal Procedure and the All Writs Act (28 U.S.C. § 1651). The courts of appeals in seven circuits, while recognizing that video surveillance does not fall within the letter of Title III, require that applications to use video surveillance of suspected criminal activities meet most of the higher constitutional standards required under Title III. Therefore, the application and order should be based on an affidavit that establishes probable cause to believe that evidence of a federal crime will be obtained by the surveillance, and should also include: (1) a statement indicating that normal investigative procedures have been tried and failed or reasonably appear to be unlikely to succeed if tried or are too dangerous; (2) a particularized description of the premises to be surveilled; (3) the names of the persons to be surveilled, if known; (4) a statement of the steps to be taken to ensure that the surveillance will be minimized to effectuate only the purposes for which the order is issued; and (5) a statement of the duration of the order, which shall not be longer than is necessary to achieve the objective of the authorization, or in any event no longer than thirty days (a ten-day grace period is not permitted; the time period begins to run from the date of the order). United States v. Williams, 124 F.3d 411 (3d Cir. 1997); United States v. Falls, 34 F.3d 674 (8th Cir. 1994); United States v. Koyomejian, 970 F.2d 536 (9th Cir.)(en banc), cert. denied, 506 U.S. 1005 (1992); United States v. Mesa-Rincon, 911 F.2d 1433 (10th Cir. 1990); United States v. Cuevas-Sanchez, 821 F.2d 248 (5th Cir. 1987); United States v. Biasucci, 786 F.2d 504 (2d Cir. 1986), cert. denied, 479 U.S. 827 (1986); United States v. Torres, 751 F.2d 875 (7th Cir. 1984), cert. denied sub nom. Rodriquez v. United States, 470 U.S. 1087 (1985).

When the government wants to intercept oral communications as well as video images within the same target premises, the same affidavit may be used to establish probable cause for the use of the microphone and the camera. Separate applications and orders, however, should be filed for each type of interception because each is governed by a different standard, and the pleadings should reflect this difference. As noted above, Title III regulates the interception of oral communications (as well as wire and electronic), and Rule 41 and the body of case law cited above establish the parameters in which video surveillance may be used for law enforcement purposes.

Consensual video surveillance does not violate the Fourth Amendment and, therefore, no court order is required. United States v. Jackson, 213 F.3d 1269 (10th Cir. 2000) (FBI installed remotely controlled cameras on the tops of telephone poles overlooking defendants' residences, and also used a "video car" equipped with three hidden cameras, two VCRs and a transmitter to

record and listen to conversations in and around the car with the consent of an informant who was a party to those communications); United States v. Cox, 836 F. Supp. 1189 (D. Md. 1993)(cooperating defendant consented to video monitoring of motel room, was in the room at all times, and the surveillance did not pick up any words or actions that were outside the consenting party's hearing and sight).

XVIII. CONSENSUAL MONITORING

1. Consensual Monitoring by Law Enforcement

Neither Title III (18 U.S.C. § 2511(2)©) nor the Fourth Amendment prohibits a law enforcement officer or a person acting under color of law[4] from intercepting a wire, oral, or electronic communication without a court order when one of the parties to the communication has consented to the interception. See United States v. Caceres, 440 U.S. 741 (1979); United States v. White, 401 U.S. 745 (1971); United States v. McKneely, 69 F.3d 1067 (10th Cir. 1995)(cooperating defendant voluntarily consented to audio and video surveillance of her hotel room); United States v. Laetividal-Gonzalez, 939 F.2d 1455 (11th Cir. 1991)(undercover agent could consent to recording of conversation with defendant), cert. denied, 503 U.S. 912 (1992); United States v. Miller, 720 F.2d 227 (1st Cir. 1983)(defendant knew cooperating witness was listening in on three-way conference call), cert. denied, 464 U.S. 1073 (1984); United States v. Shields, 675 F.2d 1152 (11th Cir.)(government properly intercepted conversations by way of a tape recorder installed by cooperating detective at the request of the defendant), cert. denied, 459 U.S. 858 (1982); United States v. Cox, 836 F. Supp. 1189 (D. Md. 1993)(cooperating defendant consented to audio and video surveillance of his motel room).

Compare these cases with United States v. Kim, 803 F. Supp. 352 (D. Hawaii 1992)(holding that the agent was not a party to the communication) and United States v. Shabazz, 883 F. Supp. 422 (D. Minn. 1995)(citing United States v. Padilla, 520 F.2d 526 (1st Cir. 1975), the court held that the informant had no right

---

[4] Courts have held repeatedly that informants who tape-record private conversations at the direction of government investigators are "acting under color of law" within the meaning of section 2511(2)(c). See United States v. Andreas, 216 F.3d 645 (7th Cir. 2000)(CW's taping of coconspirators was very loosely supervised by FBI); United States v. McKneely, 69 F.3d 1067 (10th Cir. 1995)(cooperating defendant consented to audio and video surveillance of her hotel room); Obron Atlantic Corporation v. Barr, 990 F.2d 861 (6th Cir. 1993)(continuous but irregular contact with DOJ attorneys following their request for assistance and their instructions on how to conduct the calls); United States v. Haimowitz, 725 F.2d 1561 (11th Cir.)(FBI "supervised" the taping conducted by the informant), cert. denied, 469 U.S. 1072 (1984).

to consent to the placement of recording devices in the subject's hotel room; the court was concerned that the government was free to surveil at will).

The Department has developed guidelines for the investigative use of consensual electronic surveillance in certain situations. These guidelines, which are set forth in full in the USAM, Chapter 9, Title 7, require that in certain, specified sensitive situations, law enforcement agencies must obtain advance authorization from the Department before employing consensual monitoring. The guidelines cover the investigative use of devices that intercept and record certain consensual, verbal conversations when a body transmitter or recorder, or a fixed location transmitter or recorder, is used during a face-to-face conversation. The guidelines do not apply to consensual monitoring of telephone conversations or radio transmissions. It was left to the law enforcement agencies to develop adequate internal guidelines for the use of those types of consensual monitoring.

2. Consensual Monitoring by Private Parties

Under 18 U.S.C. § 2511(2)(d), an individual may intercept an oral, wire, or electronic communication if that person is a party to the communication or a party to the communication has given consent,[5] provided the interception was not made for a criminal or tortious purpose.

A person seeking to suppress a consensual tape recording bears the burden of proving by a preponderance of the evidence that the defendant's primary motivation, or a determinative factor in the defendant's motivation, for intercepting the conversation was to commit a criminal, tortious, or other injurious act. See Sussman v. American Broadcasting Companies, Inc., 186 F.3d 1200 (9th Cir. 1999)("Prime Time Live" investigation of company providing psychic advice by telephone); Deteresa v. American Broadcasting Companies, Inc., 121 F.3d 460 (9th Cir. 1997)(interview of stewardess who worked O.J. Simpson's Chicago flight); Desnick v. American Broadcasting Companies, Inc., 44 F.3d 1345 (7th Cir. 1995)(broadcaster's use of test patients with concealed cameras to investigate clinic did not violate federal law); United States v. Zarnes, 33 F.3d 1454 (7th

[5] Williams v. Poulos, 11 F.3d 271 (1st Cir. 1993)(while the employee was advised of monitoring, it was not clear that he was told about the manner in which the monitoring would be conducted and that he would be subject to monitoring; consent was not implied); Griggs-Ryan v. Smith, 904 F.2d 112 (1st Cir. 1990)(plaintiff was warned several times that all calls would be monitored); Watkins v. L.M. Berry & Co., 704 F.2d 577 (11th Cir. 1983)(knowledge of monitoring capability does not result in implied consent).

Cir. 1994)(ex-wife made tape for the lawful purpose of potentially seeking leniency with the government), cert. denied, 515 U.S. 1126 (1995); United States v. Cassiere, 4 F.3d 1006 (1st Cir. 1993)(tape was made "to prevent future distortions by a participant"); United States v. Underhill, 813 F.2d 105 (6th Cir.)("the legality of an interception is determined by the purpose for which the interception is made, not by the subject of the communications intercepted"), cert. denied, 484 U.S. 821 (1987).

The fact that the consenting party may have violated state law requiring consent by all parties does not, by itself, establish that the consenting party intercepted the conversations for the purpose of committing any criminal or tortious act in violation of the state law. "Thus, the focus is not upon whether the interception itself violated another law; it is upon whether the purpose for the interception--its intended use-was criminal or tortious. To hold otherwise would result in the imposition of liability under the federal statute for something that is not prohibited by the federal statute (i.e., recording a conversation with the consent of only one party), simply because the same act is prohibited by a state statute. Surely this is not the result intended by Congress." Payne v. Norwest Corporation, 911 F. Supp. 1299 (D. Mont. 1995). See also Sussman v. American Broadcasting Company, Inc., 186 F.3d 1200 (9th Cir. 1999); Glinski v. City of Chicago, 2002 WL 113884 (N.D. Ill.)(citing Sussman); Roberts v. Americable Intern. Inc., 883 F. Supp. 499 (E.D. Cal. 1995); United States v. DiFelice, 837 F. Supp. 81 (S.D.N.Y. 1993).

XIX. CUSTODIAL MONITORING

1. Law Enforcement Access to Monitored Prison Calls

In 1987, the Criminal Division established guidelines for the Bureau of Prisons (BOP) on law enforcement access to electronically monitored and intercepted inmate telephone calls. In short, the Division requires law enforcement to obtain a court order or a subpoena to obtain inmate telephone calls in connection with a criminal investigation. While this requirement seemingly exceeds the legal requirements regarding law enforcement access to monitored prison calls, it ensures BOP's future ability to monitor inmate calls by diminishing the risk that access to them will not exceed the bounds of propriety. By not testing the courts' tolerance of inmate monitoring, the Division is protecting the monitoring program. In addition, the requirement of a court order or subpoena protects the privacy interests of members of the public who have a privacy interest in their phone calls and the arguable privacy interest that inmates may have in personal calls which do not implicate prison security. See United States v. Green, 842 F. Supp. 68 (W.D.N.Y.

1994)(recordings focused on a particular inmate and made to gather evidence for a criminal investigation was not monitoring in the ordinary course of business; tapes nevertheless admissible under theory of implied consent), cert. denied, 117 S. Ct. 373 (1996); Langton v. Hogan, 71 F.3d 930 (1st Cir. 1995)(debatable whether implied consent can be given freely and voluntarily in a prison setting). See also an opinion by the Office of Legal Counsel (OLC), dated January 14, 1997, in which OLC cautioned that the monitoring of a particular inmate's telephone calls for purposes unrelated to prison security or administration "may jeopardize the application of the ordinary course of duties exception" to Title III. OLC stated further that such a result would be "fatal in jurisdictions that reject the implied consent theory of monitoring."

Briefly, the Division's policy is as follows: in the event that a telephone conversation, monitored routinely by prison officials for the purpose of prison security, is found to contain information relating to the violation of federal or state law, prison officials may disclose that information to the proper law enforcement authorities for further investigation and/or prosecution. Law enforcement authorities outside the Bureau of Prisons should not be allowed random access to inmate monitored telephone calls, past, present or future.

In those cases when outside law enforcement agencies request Bureau of Prisons officials to disclose transcripts of the general telephone conversations of inmates that have been monitored in the past in connection with a criminal investigation being conducted of activities outside the confines of the prison, and the request concerns specified individuals, the information requested should be disclosed only pursuant to a grand jury subpoena or other process.

In those cases when outside law enforcement agencies ask Bureau of Prisons officials to monitor and disclose the future telephone conversations of specified inmates in connection with a criminal investigation being conducted of activities outside the confines of the prison, not affecting prison security or administration, this monitoring should be conducted only when an interception order has been procured under the authority of Title III.

2. Case Law on Custodial Monitoring

The courts have upheld warrantless monitoring of a prisoner's telephone conversations under one of two theories,

consent (18 U.S.C. § 2511(2)©)[6] or the law enforcement exception (18 U.S.C. § 2510(5)(a)).[7] Occasionally, the courts have held that neither exception applies. See Campiti v. Walonis, 611 F.2d 387 (1st Cir. 1979)(holding police officer civilly liable after finding that no exception applied to situation when police officer used an extension telephone to intercept calls between inmates); In re State Police Litigation, 888 F. Supp. 1235 (D. Conn. 1995)(improper to record telephone calls to and from state police barracks when neither caller consented to the recording).

In most custodial settings, inmates and police officers will not be able to argue successfully that a reasonable expectation of privacy exists in face-to-face conversations. See United States v. Turner, 209 F.3d 1198 (10th Cir. 2000)(no reasonable expectation of privacy in a marked police car regardless of person's custodial status); Siripongs v. Calderon, 35 F.3d 1308 (9th Cir. 1994)(surreptitious tape recording of defendant's side of a telephone conversation did not violate Title III); United States v. Clark, 22 F.3d 799 (8th Cir. 1994)(marked police car); Angel v. Williams, 12 F.3d 786 (8th Cir. 1993)(police officers did not have a reasonable expectation of privacy that their conversations with an inmate in a public jail would not be intercepted); United States v. McKinnon, 985 F.2d 525 (11th Cir. 1993)(marked police car); Gross v. Taylor, 1997 WL 535872 (E.D. Pa.)(police officers on duty in patrol car do not have a reasonable expectation of privacy or non-interception); United States v. Veilleux, 846 F. Supp. 149 (D.N.H. 1994)(prisoner had no reasonable expectation of privacy in his holding cell and one-sided telephone conversations, which were overheard by guarding officer who was within earshot).

---

[6] 18 U.S.C. § 2511(2)(c)("It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties has given prior consent to such interception."). See also United States v. Footman, 215 F.3d 145 (1st Cir. 2000); United States v. Workman, 80 F.3d 688 (2d Cir. 1996); United States v. Van Poyck, 77 F.3d 285 (9th Cir. 1996); United States v. Horr, 963 F.2d 1124 (8th Cir. 1992); United States v. Hammond, 286 F.3d 189 (4th Cir. 2002).

[7] 18 U.S.C. § 2510(5)(a)("electronic, mechanical, or other device" means any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than (a) any telephone or telegraph instrument, equipment or facility, or any component thereof... (ii) being used ... by an investigative or law enforcement officer in the ordinary course of his duties"). See also Smith v. U.S. Department of Justice, 251 F.3d 1047 (D.C. Cir. 2001); United States v. Van Poyck, 77 F.3d 285 (9th Cir. 1996); United States v. Sababu, 891 F.2d 1308 (7th Cir. 1989); United States v. Paul, 614 F.2d 115 (6th Cir. 1980); United States v. Hammond, 286 F.3d 189 (4th Cir. 2002); United States v. Noriega, 764 F. Supp. 1480 (S.D. Fla. 1991).

SAMPLES

Application for Wire and/or Oral Interceptions

UNITED STATES DISTRICT COURT
_____DISTRICT OF_____

_____
)
IN THE MATTER OF THE APPLICATION)
OF THE UNITED STATES OF AMERICA FOR)
AN ORDER AUTHORIZING THE INTERCEPTION)
OF (WIRE) (ORAL) COMMUNICATIONS)
_____)

APPLICATION FOR INTERCEPTION OF (WIRE)(ORAL) COMMUNICATIONS

_____, Assistant United States Attorney, _____ District of _____, being duly sworn, states:

1. I am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code, that is, an attorney authorized by law to prosecute or participate in the prosecution of offenses enumerated in Section 2516 of Title 18, United States Code.

2. This application is for an order pursuant to Section 2518 of Title 18, United States Code, authorizing the interception of (wire) (oral) communications until the attainment of the authorized objectives or, in any event, at the end of thirty (30) days from the earlier of the day on which the investigative or law enforcement officers first begin to conduct an interception under the Court's order or ten (10) days after the order is entered, of (list those persons who will be intercepted over the telephone or within the premises, "interceptees") and others as yet unknown (if wire: "to and from the telephone(s) bearing the number(s) _____, subscribed to by _____ and located at/billed to _____") (if oral: "occurring inside the premises located at _____" or "occurring in and around a (describe the make, color and year of the vehicle) bearing the license plate number _____ and the vehicle identification number _____") concerning offenses enumerated in Section 2516 of Title 18, United States Code, that is, offenses involving violations of (list section(s) of the U.S.

Code and describe briefly the applicable offense(s)) that are being committed by (list the interceptees and those persons who are also part of the conspiracy but may not necessarily be intercepted over the target facility or within the target premises/vehicle, collectively they are referred to as "violators,") and others as yet unknown.

3. Pursuant to Section 2516 of Title 18, United States Code, the Attorney General of the United States has specially designated the Assistant Attorney General, any Acting Assistant Attorney General, any Deputy Assistant Attorney General or any acting Deputy Assistant Attorney General of the Criminal Division (or, in the case of a roving interception, the Assistant Attorney General or Acting Assistant Attorney General in the Criminal Division) to exercise the power conferred on the Attorney General by Section 2516 of Title 18, United States Code, to authorize this Application. Under the power designated to him by special designation of the Attorney General pursuant to Order Number (currently 2407-2001) of (currently March 8, 2001), an appropriate official of the Criminal Division, (insert official's name and title), has authorized this Application. Attached to this Application are copies of the Attorney General's order of special designation and the Memorandum of Authorization approving this Application.

4. I have discussed all of the circumstances of the above offenses with Special Agent _____ of the (name the investigative agency), who has directed and conducted this investigation and have examined the Affidavit of Special Agent _____, which is attached to this Application and is incorporated herein by reference. Based upon that Affidavit, your applicant states upon information and belief that:

a. there is probable cause to believe that (list the violators) and others as yet unknown have committed, are committing, and will continue to commit violations of (list the offenses - must be enumerated in Section 2516 of Title 18, United States Code);

b. there is probable cause to believe that particular (wire) (oral) communications of (name the interceptee(s)) concerning the above-described offenses will be obtained through the interception of (wire) (oral) communications. In particular, these (wire) (oral) communications will concern the (characterize the types of criminal communications expected to be intercepted). In addition, the communications are expected to constitute admissible evidence of the commission of the above-stated offenses;

c. normal investigative procedures have been tried and failed, reasonably appear to be unlikely to succeed if tried, or are too dangerous to employ, as is described in further detail in the attached Affidavit;

d. there is probable cause to believe that (identify fully the telephone(s) from which, or the premises where, the wire or oral communications are to be intercepted) is/are being used and will continue to be used in connection with the commission of the above-described offenses.

(If a roving interception, add the following language:

"The attached affidavit contains information demonstrating, within the meaning of Title 18, United States Code, Section 2518 (11)(a) and/or (b), that (if oral: "specification of the place(s) where communications of (name the interceptees) are to be intercepted is not practical") (if wire: "that (name the person(s))use of various and changing facilities could have the effect of thwarting interception from a specified facility")).

5. The attached Affidavit contains a full and complete statement of facts concerning all previous applications which are known to have been made to any judge of competent jurisdiction for approval of the interception of the oral, wire or electronic communications of any of the same individuals, facilities, or premises specified in this Application. (If there has been no previous electronic surveillance, state: "The applicant is aware of no previous applications made to any judge for authorization to intercept the oral, wire or electronic communications of any of the persons or involving the (facilities) (premises) specified in this application.")

WHEREFORE, your applicant believes that there is probable cause to believe that (name the violators) and others as yet unknown are engaged in the commission of offenses involving (cite to the offenses), that (name the interceptees) and others yet unknown are using (the telephone bearing the number _____, subscribed to by _____ and located at/billed to _____) and/or (the premises or vehicle described as _____) in connection with the commission of the above-described offenses; and that (wire) (oral) communications of (name the interceptees) and others yet unknown will be intercepted (over the above-described telephone facility) and/or (within the above-described premises or the above-described vehicle).

Based on the allegations set forth in this application and on the affidavit of Special Agent _____, attached, the applicant requests this court to issue an order pursuant to the

power conferred upon it by Section 2518 of Title 18, United States Code, authorizing the (investigative agency) to intercept (wire communications to and from the above-described facility(ies)) and/or (oral communications from the above-described premises) until such communications are intercepted that reveal the manner in which the named violators and others unknown participate in the specified offenses and reveal the identities of (his)(their) coconspirators, place(s) of operation, and nature of the conspiracy, or for a period of (not to exceed 30 days) measured from the day on which the investigative or law enforcement officers first begin to conduct the interception or ten days from the date of this order, whichever occurs first.

(If interception of oral communications is requested, add:

IT IS REQUESTED FURTHER that this Court issue an order pursuant to Section 2518 of Title 18, United States Code, authorizing Special Agents of the (name investigative agency) to make all necessary surreptitious and/or forcible entries to effectuate the purposes of this Court's Order, including entries to install, maintain, and remove electronic listening devices from (describe the premises/vehicle). The applicant shall notify the Court of any surreptitious entry.)

(If interception of wire communications is requested, add:

IT IS REQUESTED FURTHER that the authorization given be intended to apply not only to the target telephone number(s) listed above, but to any changed telephone number subsequently assigned to the same cable, pair, and binding posts utilized by the target telephone(s) within the thirty (30) day period. (If the telephone is a cellular telephone, the language should state: "the authorization given be intended to apply not only to the target telephone number(s) listed above, but to any changed telephone number or any other telephone number subsequently assigned to or used by the instrument bearing the same electronic serial number as the target cellular phone within the thirty (30) day period.") It is also requested that the authorization be intended to apply to background conversations intercepted in the vicinity of the target telephone(s) while the telephone(s) is off the hook or otherwise in use.)

(If multi-jurisdictional authorization for a portable/mobile facility is requested, add:

IT IS REQUESTED FURTHER that in the event that the target facility/vehicle is transferred outside the territorial jurisdiction of this Court, interceptions may take place in any other jurisdiction within the United States.)

(If a roving interception is requested, add:

IT IS REQUESTED FURTHER that this Court issue an order authorizing the roving interception of the (wire) (oral) communications of (name the target(s)) (if wire: "from various and changing telephone facilities), (if oral: "from various locations in (name the jurisdiction) that are not practical to specify) as provided in Title 18, United States Code, Section 2518(11)(a) or (b) and as specifically authorized by the (Acting) Assistant Attorney General of the Criminal Division, for a thirty (30) day period.)

(If wire communication, add:

IT IS REQUESTED FURTHER that this Court issue an order pursuant to Section 2518(4) of Title 18, United States Code, directing the (name the communications service provider(s)), an electronic communications service provider as defined in Section 2510(15) of Title 18, United States Code, to furnish and continue to furnish the (investigative agency) with all information, facilities and technical assistance necessary to accomplish the interceptions unobtrusively and with a minimum of interference with the services that such providers are according the persons whose communications are to be intercepted, and to ensure an effective and secure installation of electronic devices capable of intercepting wire communications over the above-described telephone. The service provider shall be compensated by the Applicant for reasonable expenses incurred in providing such facilities or assistance.)

IT IS REQUESTED FURTHER, to avoid prejudice to this criminal investigation, that the Court order the providers of electronic communication service and their agents and employees not to disclose or cause a disclosure of this Court's Order or the request for information, facilities, and assistance by the (investigative agency) or the existence of the investigation to any person other than those of their agents and employees who require this information to accomplish the services requested. In particular, said providers and their agents and employees should be ordered not to make such disclosure to a lessee, telephone subscriber, or any interceptee or participant in the intercepted communications.

IT IS REQUESTED FURTHER that this Court direct that its Order be executed as soon as practicable after it is signed and that all monitoring of (wire) (oral) communications shall be conducted in such a way as to minimize the interception and disclosure of the communications intercepted to those communications relevant to the pending investigation, in accordance with the minimization requirements of Chapter 119 of

Title 18, United States Code. The interception of (wire) (oral) communications authorized by this Court's Order must terminate upon attainment of the authorized objectives or, in any event, at the end of thirty (30) days measured from the day on which investigative or law enforcement officers first begin to conduct an interception or ten (10) days after the Order is entered.

Monitoring of conversations must immediately terminate when it is determined that the conversation is unrelated to communications subject to interception under Chapter 119 of Title 18, United States Code. Interception must be suspended immediately when it is determined through voice identification, physical surveillance, or otherwise, that none of the named interceptees or any of their confederates, when identified, are participants in the conversation unless it is determined during the portion of the conversation already overheard that the conversation is criminal in nature.

IT IS REQUESTED FURTHER that the Court order that either (Applicant/AUSA) or any other AUSA familiar with the facts of the case provide the Court with a report on or about the (tenth), (twentieth) and (thirtieth) days following the date of this Order showing what progress has been made toward achievement of the authorized objectives and the need for continued interception. If any of the aforementioned reports should become due on a weekend or holiday, it is requested further that such report become due on the next business day thereafter.

IT IS REQUESTED FURTHER that the Court order that its Orders, this application and the accompanying affidavit and proposed Order(s), and all interim reports filed with the Court with regard to this matter be sealed until further order of this Court, except that copies of the Order(s), in full or redacted form, may be served on the (name the investigative agency/agencies) and the service provider(s) as necessary to effectuate the Court's Order as set forth in the proposed order(s) accompanying this application.

DATED this _____ day of _____, 20__.
(Name and title of the applicant)

_____
(NAME)
Assistant United States Attorney

SUBSCRIBED and SWORN to before me
this _____ day of _____, 20__.

_____
UNITED STATES DISTRICT COURT JUDGE
(District)

Affidavit for Oral and/or Wire Interception

UNITED STATES DISTRICT COURT
_____DISTRICT OF_____

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER AUTHORIZING THE INTERCEPTION OF (WIRE) (ORAL) COMMUNICATIONS	)

AFFIDAVIT IN SUPPORT OF APPLICATION

INTRODUCTION

_____, being duly sworn, deposes and states as follows:

1. I am a Special Agent with the _____, United States Department of Justice. I have been so employed by the (name the agency) for the past _____ ( ) years. I have participated in investigations involving (organized crime/drug trafficking/money laundering, etc.) activities for the past _____ ( ) years. (Describe present assignment.)

2. I am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code, and am empowered by law to conduct investigations and to make arrests for offenses enumerated in Section 2516 of Title 18, United States Code.

3. This affidavit is submitted in support of an application for an order authorizing the interception of (wire)(oral) communications occurring (describe the facility or premises to which the application and affidavit are directed).

4. I have participated in the investigation of the above offenses. As a result of my personal participation in this investigation, through interviews with and analysis of reports submitted by other (Special Agents of the _____ and/or other state/local law enforcement personnel), I am familiar with all aspects of this investigation. On the basis of this familiarity, and on the basis of other information which I have reviewed and determined to be reliable, I allege the facts to show that:

a. there is probable cause to believe that (name the violators) are committing, and will continue to commit violations of (list the offenses - must be ones enumerated in Section 2516 of Title 18, United States Code);

b. there is probable cause to believe that particular (wire)(oral) communications of (name the interceptees) concerning the above offenses will be obtained through the interception of such communications (if wire: "to and from the telephone(s) bearing the number(s) _____, subscribed to by _____ and located at/billed to _____"; if oral: "occurring within premises located at _____" or "occurring in and around a (indicate the make, model and year of the vehicle) bearing the license plate _____ and vehicle identification number _____"); if a roving wire interception: "over various and changing facilities within (identify the jurisdiction) used by (name the particular interceptee(s)- do not include the language "and others yet unknown"); if a roving oral interception: "within presently unknown premises used by (name the particular interceptee(s) - do not include the language "and others yet unknown") that it is impractical to specify.").

In particular, these communications are expected to concern the specifics of the above offenses, including (I) the nature, extent and methods of the (describe the illegal activity) business of (name the violators) and others; (ii) the nature, extent and methods of operation of the business of (name the violators) and others; (iii) the identities and roles of accomplices, aiders and abettors, co-conspirators and participants in their illegal activities; (iv) the distribution and transfer of the contraband and money involved in those activities; (v) the existence and location of records; (vi) the location and source of resources used to finance their illegal activities; (vii) the location and disposition of the proceeds from those activities; and (viii) the locations and items used in furtherance of those activities. In addition, these (wire)(oral) communications are expected to constitute admissible evidence of the commission of the above-described offenses.

The statements contained in this affidavit are based in part on information provided by Special Agents of the (name the investigative agency/agencies), on conversations held with detectives and officers from the (identify the local/state police department), on information provided by confidential sources, and on my experience and background as a Special Agent of the _____. Since this affidavit is being submitted for the limited purpose of securing authorization for the interception of (wire)(oral) communications, I have not included each and every fact known to me concerning this investigation. I have set forth

only the facts that I believe are necessary to establish the necessary foundation for an order authorizing the interception of (oral)(wire) communications.

PERSONS EXPECTED TO BE INTERCEPTED

Include a short description of each known violator; if appropriate, explain why certain participants in the offenses are not expected to be interceptees. If applicable, note which persons are currently facing pending state or federal criminal charges.

FACTS AND CIRCUMSTANCES

Provide an in-depth discussion of the facts in support of the probable cause statements set forth above. If informant information provides a basis for any of the required information, provide adequate qualifying language for each informant. Remember that you must show probable cause 1) that the alleged offenses are being committed; 2) that the named subjects and others unknown are committing them; and 3) that the targeted telephone(s) and/or premises is/are being used to commit these offenses. It is Department of Justice policy that pen register or telephone toll information for the target telephone(s), or physical surveillance of the targeted premises, standing alone, is generally insufficient to establish probable cause. Probable cause to establish criminal use of the facilities or premises requires independent evidence of use in addition to pen register or surveillance information, e.g. informant or undercover information. On rare occasions, criminal use of the target facilities or premises may be established by an extremely high volume of calls to other known or suspected coconspirators that coincides with incidents of illegal activity, or by a regular pattern of telephone or premises use involving known or suspected coconspirators going back for a period of years.

When requesting a roving wire interception, you must establish that the specifically targeted subject uses various and changing facilities in such a way that has the effect of thwarting law enforcement's ability to intercept the subject's communications from a specified facility. See 18 U.S.C. § 2518(11)(b)(ii). The effect on the government's ability to intercept a subject's calls can be demonstrated by the subject's actions over a period of time (e.g., physical surveillance and phone record analysis establishing that the subject travels from pay phone to pay phone to call other coconspirators, or the analysis of phone records demonstrating that the subject uses different cellular phones in succession for brief periods of time (usually three weeks or less) to contact other coconspirators, in furtherance of criminal activity). Roving wiretaps will be

authorized for public and cellular telephones only, and only when it is clear that the telephones cannot be identified in advance, and that the subject's actions are having the effect of preventing the government from conducting interceptions over his phones.

In roving oral interceptions (see 18 U.S.C. § 2518(11)(a)(ii)), you must establish probable cause that it is not practical to specify the place where the oral communications of the targeted individual(s) are to be intercepted. Once again, a roving oral interception will generally be authorized only for public facilities, vehicles, hotel rooms, or similar locations, and a pattern of activity demonstrating the impracticability of naming specific premises must be established.

NEED FOR INTERCEPTION

Need for (Wire)(Oral) Interception

Based upon your affiant's training and experience, (as well as the experience of the other (Special Agents of the _____ and/or state/local officers), and based upon all of the facts set forth herein, it is your affiant's belief that the interception of (wire)(oral) communications is the only available technique that has a reasonable likelihood of securing the evidence necessary to prove beyond a reasonable doubt that (name the violators), and others as yet unknown are engaged in the above-described offenses.

Your affiant states that the following investigative procedures, which are usually employed in the investigation of this type of criminal case, have been tried and have failed, reasonably appear to be unlikely to succeed if they are tried, or are too dangerous to employ.

ALTERNATIVE INVESTIGATIVE TECHNIQUES

Physical Surveillance

(The following is an example of language that discusses the use of physical surveillance in general; you should also discuss the effectiveness of this, and the following other investigative techniques, as they are applicable to your particular case.)

Physical surveillance has been attempted on numerous occasions during this investigation. Although it has proven valuable in identifying some activities and associates of (list the violators), physical surveillance, if not used in conjunction with other techniques, including electronic surveillance, is of limited value. Physical surveillance, even if highly successful,

has not succeeded in gathering sufficient evidence of the criminal activity under investigation. Physical surveillance of the alleged conspirators will not (has not) established conclusively the elements of the violations and has not and most likely will not establish conclusively the identities of various conspirators. In addition, (continued) surveillance is not expected to enlarge upon information now available; rather, such prolonged or regular surveillance of the movements of the suspects would most likely be noticed, causing them to become more cautious in their illegal activities, to flee to avoid further investigation and prosecution, to cause a real threat to the safety of the informant(s) and undercover agent(s), or to otherwise compromise the investigation.

Physical surveillance is also unlikely to establish conclusively the roles of the named conspirators, to identify additional conspirators, or otherwise to provide admissible evidence in regard to this investigation because (discuss any of the following which are applicable to the case):

- the subjects are using counter-surveillance techniques, such as erratic driving behavior, or have evinced that they suspect that law enforcement surveillance is being conducted against them; and/or

- it is not possible to determine the full nature and scope of the aforementioned offenses by the use of physical surveillance; and/or

- the nature of the neighborhood forecloses physical surveillance; (e.g., close-knit community, physical location (cul-de-sac, dead-end, large apartment building), observant neighbors); and/or

- further surveillance would only serve to alert the suspects of the law enforcement interest in their activities and compromise the investigation.

Use of Grand Jury Subpoenas

Based upon your affiant's experience and conversations with Assistant United States Attorney _____, who has experience prosecuting violations of criminal law, your affiant believes that subpoenaing persons believed to be involved in this conspiracy and their associates before a Federal Grand Jury would not be completely successful in achieving the stated goals of this investigation. If any principals of this conspiracy, their co-conspirators and other participants were called to testify before the Grand Jury, they would most likely be uncooperative and invoke their Fifth Amendment privilege not to testify. It

would be unwise to seek any kind of immunity for these persons, because the granting of such immunity might foreclose prosecution of the most culpable members of this conspiracy and could not ensure that such immunized witnesses would provide truthful testimony. Additionally, the service of Grand Jury subpoenas upon the principals of the conspiracy or their co-conspirators would only (further) alert them to the existence of this investigation, causing them to become more cautious in their activities, to flee to avoid further investigation or prosecution, to threaten the lives of the informant(s) and the undercover agent(s), or to otherwise compromise the investigation.

(Add specific information regarding any persons who have been subpoenaed before the Grand Jury, especially when the Fifth Amendment was invoked or when the witness later advised the targets.)

Confidential Informants and Cooperating Sources

Reliable confidential informants/cooperating sources have been developed and used, and will continue to be developed and used, in regard to this investigation. However, these sources (discuss only those that are applicable):

- exist on the fringe of this organization and have no direct contact with mid- or high-level members of the organization, or such contact is virtually impossible because the sources have no need to communicate with such individuals; and/or

- refuse to testify before the Grand Jury or at trial because of fear of personal or family safety, or their testimony would be uncorroborated or otherwise would be subject to impeachment (due to prior record, criminal involvement, etc.); and/or

- are no longer associated with the subjects of this investigation (and their information is included for historical purposes only); and/or

- are unable to furnish information which would identify fully all members of this ongoing criminal conspiracy or which would define the roles of those conspirators sufficiently for prosecution.

(In addition, discuss whether the information provided by the confidential sources, even if all sources agreed to testify, would not, without the requested electronic surveillance, result in a successful prosecution of all of the participants.)

Undercover Agents

Undercover agents have been unable to infiltrate the inner workings of this conspiracy due to the close and secretive nature of this organization. Your affiant believes that there are no undercover agents who can infiltrate the conspiracy at a level high enough to identify all members of the conspiracy or otherwise satisfy all the goals of this investigation. (Indicate if infiltration is not feasible because the confidential informant(s) is not in a position to make introductions of undercover agents to mid- or high-level members of the organization.)

(Details of the use of undercover agents should have been provided in the body of the affidavit, with this section indicating the limitations of such use.)

Interviews of Subjects or Associates

Based upon your affiant's experience, I believe that interviews of the subjects or their known associates would produce insufficient information as to the identities of all of the persons involved in the conspiracy, the source of (the drugs, financing, etc.), the location of (records, drugs, etc.), and other pertinent information regarding the named crimes. Your affiant also believes that any responses to the interviews would contain a significant number of untruths, diverting the investigation with false leads or otherwise frustrating the investigation. Additionally, such interviews would also have the effect of alerting the members of the conspiracy, thereby compromising the investigation and resulting in the possible destruction or concealment of documents and other evidence, and the possibility of harm to cooperating sources whose identities may become known or whose existence may otherwise be compromised.

(This portion of the affidavit is sometimes merged with the discussion regarding the use of the Federal Grand Jury. Any actual interviews conducted, and any resulting problems, should also be discussed here.)

Search Warrants

The execution of search warrants in this matter has been considered. However, use of such warrants would, in all likelihood, not yield a considerable quantity of (narcotics, money, or other identified contraband) or (relevant documents) nor would the searches be likely to reveal the total scope of the illegal operation and the identities of the co-conspirators. (It is unlikely that all, or even many, of the principals of this

organization would be at any one location when a search warrant was executed.) The affiant believes that search warrants executed at this time would be more likely to compromise the investigation by alerting the principals to the investigation and allowing other unidentified members of the conspiracy to insulate themselves further from successful detection.

Pen Registers/Telephone Toll Records/Traps and Traces

Pen register (and/or trap and trace) information has been used in this investigation, including pen register(s) (and/or traps and traces) on the target telephone(s), as described above. The pen register (and/or trap and trace) information has verified frequent telephone communication between the target telephone(s) and other telephones. Pen registers (and/or traps and traces), however, do not record the identity of the parties to the conversation, cannot identify the nature or substance of the conversation, or differentiate between legitimate calls and calls for criminal purposes. A pen register (and/or trap and trace) cannot identify the source or sources of the controlled substances, nor can it, in itself, establish proof of the conspiracy. Telephone toll information, which identifies the existence and length of telephone calls placed from the target telephone to telephones located outside of the local service zone, has the same limitations as pen registers (and/or traps and traces), does not show local calls, and is generally available only on a monthly basis.

Other Limitations

(Provide details concerning violence, such as murdered or hurt witnesses, threats, etc., and other situations present in your investigation that limit the effectiveness of normal investigative techniques.)

Based upon the foregoing, it is your affiant's belief that the interception of (wire)(oral) communications is an essential investigative means in obtaining evidence of the offenses in which the subject(s) and others as yet unknown are involved.

PRIOR APPLICATIONS

Based upon a check of the records of the (Federal Bureau of Investigation, the Drug Enforcement Administration, and any other appropriate agency), no prior federal applications for an order authorizing or approving the interception of wire, oral, or electronic communications have been made involving the persons, premises or facilities named herein. (If the facts warrant, include additional information concerning prior or ongoing electronic surveillance, including the dates of the interception,

the jurisdiction where the order was signed and the relevance, if any, to the instant application. While there is no obligation to conduct a search of state law enforcement electronic surveillance indices, information about prior state taps must be included if the government has knowledge of them through other means.)

MINIMIZATION

All interceptions will be minimized in accordance with the minimization requirements of Chapter 119 of Title 18, United States Code, and all interceptions conducted pursuant to this Court's Order will terminate upon attainment of the authorized objectives or, in any event, at the end of thirty (30) days measured from the earlier of the day on which investigative or law enforcement officers first begin to conduct an interception under the Court's Order or ten (10) days after the Order is entered. Monitoring of conversations will terminate immediately when it is determined that the conversation is unrelated to communications subject to interception under Chapter 119 of Title 18, United States Code. Interception will be suspended immediately when it is determined through voice identification, physical surveillance, or otherwise, that none of the named interceptees or any of their confederates, when identified, are participants in the conversation, unless it is determined during the portion of the conversation already overheard that the conversation is criminal in nature. (If pertinent, add additional language concerning the use of foreign languages and other minimization considerations particular to the case, such as targeting the use of public facilities or premises or non-interception of privileged communications of interceptees who have pending criminal charges.)

_____
(NAME)
Special Agent
(Agency)

Sworn to before me this
_____ day of _____, 20__.

_____
UNITED STATES DISTRICT COURT JUDGE
(District)

Order for Interception of Wire and/or Oral Communications

UNITED STATES DISTRICT COURT
_____ DISTRICT _____

_____
)
IN THE MATTER OF THE APPLICATION)
OF THE UNITED STATES OF AMERICA FOR)
AN ORDER AUTHORIZING THE INTERCEPTION)
OF (WIRE)(ORAL) COMMUNICATIONS)
_____)

ORDER AUTHORIZING THE INTERCEPTION OF (WIRE)
(ORAL) COMMUNICATIONS

Application under oath having been made before me by _____, Assistant United States Attorney, _____ District of _____, an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code, for an Order authorizing the interception of (wire)(oral) communications pursuant to Section 2518 of Title 18, United States Code, and full consideration having been given to the matter set forth therein, the Court finds:

(the following lettered paragraphs should be virtually identical to the probable cause paragraphs contained in the application and affidavit)

a. there is probable cause to believe that (list the violators) have committed, and are committing, and will continue to commit violations of (list the offenses - must be ones enumerated in Section 2516 of Title 18, United States Code);

b. there is probable cause to believe that particular (wire)(oral) communications of (name the interceptees) concerning the above-described offenses will be obtained through the interception for which authorization has herewith been applied. In particular, there is probable cause to believe that the interception of (wire communications to and from the telephone bearing the number _____, subscribed to by _____ and located at/billed to _____) (oral communications occurring in the premises located at _____ and/or in and around the vehicle described as _____), will concern the specifics of the above offenses, including the manner and means of the commission of the offenses(s); (If roving interception is

applied for: "the application has also demonstrated adequately within the meaning of Title 18, United States Code, Section 2518 (11)(a) and/or (b), that (if oral: "specification of the place(s) where the oral communications of (name the interceptee(s)) are to be intercepted is not practical")(if wire: "(name the interceptee(s)) use of various changing facilities could have the effect of thwarting interception from a specified facility.")));

c. it has been established that normal investigative procedures have been tried and have failed, reasonably appear to be unlikely to succeed if tried, or are too dangerous to employ; and

d. there is probable cause to believe that (identify the facilities from which, or the place where, the wire or oral communications are to be intercepted) have been and will continue to be used in connection with commission of the above-described offenses.

WHEREFORE, IT IS HEREBY ORDERED that Special Agents of the (name the investigative agency/agencies; also indicate if state and local officers are participating in the investigation, particularly if they will be monitors) are authorized, pursuant to an application authorized by a duly designated official of the Criminal Division, (insert official's name and title), United States Department of Justice, pursuant to the power delegated to that official by special designation of the Attorney General and vested in the Attorney General by Section 2516 of Title 18, United States Code, to intercept (wire)(oral) communications (if wire: "to and from the above-described telephone(s)") (if oral: "in the above-described premises (or vehicle).")

PROVIDED that such interception(s) shall not terminate automatically after the first interception that reveals the manner in which the alleged co-conspirators and others as yet unknown conduct their illegal activities, but may continue until all communications are intercepted which reveal fully the manner in which the above-named persons and others as yet unknown are committing the offenses described herein, and which reveal fully the identities of their confederates, their places of operation, and the nature of the conspiracy involved therein, or for a period of thirty (30) days measured from the day on which investigative or law enforcement officers first begin to conduct an interception under this order or ten (10) days after this order is entered, whichever is earlier.

(If a mobile or cellular telephone or facility, add:

IT IS ORDERED FURTHER that in the event that the target facility/vehicle is transferred outside the territorial

jurisdiction of this court, interceptions may take place in any other jurisdiction within the United States.)

(If oral communications, add:

IT IS ORDERED FURTHER that Special Agents of the (name the agency/agencies) may make all necessary surreptitious and/or forcible entries to effectuate the purposes of this order, including but not limited to entries to install, maintain and remove electronic listening devices within (describe the premises or vehicle). Applicant shall notify the Court of each surreptitious entry.)

(If interception of wire communications is requested, add:

IT IS ORDERED FURTHER that the authorization apply not only to the target telephone number(s) listed above, but to any changed telephone number subsequently assigned to the same cable, pair, and binding posts utilized by the target telephone(s) within the thirty (30) day period. (In the case of a cellular telephone: "... but to any changed telephone number or any other telephone number subsequently assigned to or used by the instrument bearing the same electronic serial number as the target cellular phone within the thirty (30) day period.") It is also ordered that the authorization apply to background conversations intercepted in the vicinity of the target telephone(s) while the telephone(s) is off the hook or otherwise in use.)

(If a roving interception is being ordered, add:

IT IS ORDERED FURTHER that the authorization to intercept (wire)(oral) communications shall include the interception of the (wire)(oral) communications of (name the interceptee(s)) ((if wire: "from various and changing telephone facilities," pursuant to 18 U.S.C. § 2518(11)(b)); (if oral: "from presently unknown premises used by (name the interceptee(s)) that it is not practical to specify, pursuant to 18 U.S.C. § 2518(11)(a)).

(If wire communications, add:

IT IS ORDERED FURTHER that, based upon the request of the Applicant pursuant to Section 2518(4) of Title 18, United States Code, the (name the communication service provider(s)), an electronic communication service provider(s) as defined in Section 2510(15) of Title 18, United States Code, shall furnish the (investigative agency) with all information, facilities and technical assistance necessary to accomplish the interceptions unobtrusively and with a minimum of interference with the services that such provider is according the persons whose

communications are to be intercepted, with the service provider(s) to be compensated by the Applicant for reasonable expenses incurred in providing such facilities or assistance.)

IT IS ORDERED FURTHER that, to avoid prejudice to the government's criminal investigation, the provider(s) of the electronic communications service and its agents and employees are ordered not to disclose or cause a disclosure of the Order or the request for information, facilities and assistance by the (investigative agency), or the existence of the investigation to any person other than those of its agents and employees who require this information to accomplish the services hereby ordered. In particular, said provider(s) and its agents and employees shall not make such disclosure to a lessee, telephone subscriber or any interceptee or participant in the intercepted communications.

IT IS ORDERED FURTHER that this order shall be executed as soon as practicable and that all monitoring of (wire)(oral) communications shall be conducted in such a way as to minimize the interception and disclosure of the communications intercepted to those communications relevant to the pending investigation. The interception of (wire)(oral) communications must terminate upon the attainment of the authorized objectives, not to exceed thirty (30) days measured from the earlier of the day on which investigative or law enforcement officers first begin to conduct an interception of this order or ten (10) days after the order is entered.

Monitoring of conversations must terminate immediately when it is determined that the conversation is unrelated to communications subject to interception under Chapter 119, Title 18, United States Code. Interception must be suspended immediately when it is determined through voice identification, physical surveillance, or otherwise, that none of the named interceptees or any of their confederates, when identified, are participants in the conversation unless it is determined during the portion of the conversation already overheard that the conversation is criminal in nature. If the conversation is minimized, the monitoring agent shall spot check to insure that the conversation has not turned to criminal matters.

IT IS ORDERED FURTHER that Assistant United States Attorney _____ or any other Assistant United States Attorney familiar with the facts of this case shall provide this Court with a report on or about the (tenth), (twentieth), and (thirtieth) days following the date of this Order showing what progress has been made toward achievement of the authorized objectives and the need for continued interception. If any of the above-ordered reports should become due on a weekend or

holiday, IT IS ORDERED FURTHER that such report shall become due on the next business day thereafter.

IT IS ORDERED FURTHER that this Order, the application, affidavit and proposed order(s), and all interim reports filed with this Court with regard to this matter, shall be sealed until further order of this Court, except that copies of the order(s), in full or redacted form, may be served on the (investigative agency/agencies) and the service provider(s) as necessary to effectuate this order.

_____
UNITED STATES DISTRICT COURT JUDGE
(District)

Dated this _____ day of _____, 20__.

Order to Service Provider

UNITED STATES DISTRICT COURT
_____ DISTRICT OF_____

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER AUTHORIZING THE INTERCEPTION OF (WIRE)(ELECTRONIC) COMMUNICATIONS	)

ORDER TO SERVICE PROVIDER

This matter comes before the Court pursuant to the Application of the United States of America for an order authorizing the interception of (wire)(electronic) communications pursuant to Title 18, United States Code, Section 2518, (if wire: "to and from the telephone(s) bearing the number(s) _____ and located at/billed to _____") (if electronic: "to and from the pager/facsimile machine/computer bearing the telephone number and located at/billed to _____").

The Court, having reviewed the Application and found that it conforms in all respects to the requirements of Title 18, United States Code, Sections 2516 and 2518, has this day signed an Order conforming to the provisions of Title 18, United States Code, Section 2518, authorizing the (name the investigative agency/agencies) to accomplish the aforesaid interception.

IT APPEARING FURTHER that the Applicant has requested that the (name the service provider(s)) be directed to furnish, and continue to furnish, the Applicant and (name the investigative agency) with all information, facilities and technical assistance necessary to accomplish the interception(s) unobtrusively and with a minimum of interference with the services such provider(s) is according the person(s) whose communications are to be intercepted, and to ensure an effective and secure installation of electronic devices capable of interception of wire communications over the above-described telephone(s) and/or electronic communications over the above-described facsimile machine/pager/computer.

IT IS HEREBY ORDERED that the (name the service provider(s)), shall furnish, and continue to furnish, the (name the investigative agency) with all information, facilities and technical assistance necessary to accomplish the interception(s)

unobtrusively and with minimum interference with the services that such provider(s) is according the person(s) whose communications are to be intercepted, and to ensure an effective and secure installation of electronic devices capable of interception of wire communications over the above-described telephone(s) and/or facsimile machine/pager/computer.

IT IS ORDERED FURTHER that the service provider(s) is to be compensated by the Applicant for reasonable expenses incurred in providing such facilities or assistance.

IT IS ORDERED FURTHER that the furnishing of said information, facilities, and technical assistance shall terminate thirty (30) days measured from the earlier of the day that assistance is provided under this order or ten (10) days from the date this Order is entered, unless otherwise ordered by this Court; and

IT IS ORDERED FURTHER that this Order is sealed, except that copies of this Order may be served on the (name the investigative agency/agencies) and (name the service provider(s)), and, to avoid prejudice to the criminal investigation, that the (name the service provider(s)) and its agents and employees shall not disclose or cause a disclosure of this Order or the request for assistance or the existence of this investigation to any person other than those of its agents and employees who require this information to accomplish the services hereby ordered, unless and until otherwise ordered by this Court. In particular, no such disclosure may be made to a lessee, telephone subscriber, or any interceptee or participant in the intercepted communications.

DATED this _____ day of _____, 20___.

_____
UNITED STATES DISTRICT COURT JUDGE
(District)

Sample Minimization Instructions
for Oral and Wire Communications

MEMORANDUM

TO: Monitoring Agents
FROM: AUSA _____
RE: Minimization Instructions
DATE: _____

1. All agents must read the affidavit, application, order and these instructions and sign these instructions before monitoring.

2. The Order of _____ only authorizes the interception of conversations of (name the interceptees listed in the Order) with anyone else occurring (to and from telephone number _____ subscribed to by _____)(at the premises known as _____ and located at _____), regarding offenses involving (list the offenses).

3. Agents may spot monitor for a reasonable period not to exceed two minutes to determine whether the subject is present and participating in a conversation. This spot monitoring may occur as often as is reasonable, but in any event at least one minute should elapse between interceptions.

4. If, during this spot monitoring, it is determined that additional individuals are engaged in criminal conversation, intercepts may continue despite the fact that the named subject is not engaged in conversations, until the conversation ends or becomes non-pertinent. If individuals other than the subject are participating in criminal conversation, continue to monitor and advise the case agent or supervisor immediately. If these individuals can be identified, provide this information also.

5. If the subject is engaged in conversation, interception may continue for a reasonable time, usually not in excess of two minutes, to determine whether the conversation concerns criminal activities.

(a) If such a conversation is unclear but may be related to (name the offenses), interception may continue until such time as it is determined that the conversation clearly no longer relates to that topic.

(b) If such a conversation is unclear but may relate to other criminal activities, interception should cease after about two minutes unless it can be determined within that time that the

conversation does in fact relate to such other criminal activities, in which case interception may continue.

6. The above instructions regarding the number of minutes of permissible interception will vary once experience has been gained. If experience shows that conversations between certain people are invariably innocent, interception of such conversations should be ended sooner. If experience shows that other individuals always discuss criminal activities, a longer interception may be justified. This is especially true for individuals who can be identified as participants with the subjects in possessing and distributing controlled substances. Read all of the logs of interceptions on a continuing basis and notify the case agent if patterns develop.

7. No conversation may be intercepted that would fall under any legal privilege. The four categories of privileged communications are described below:

(a) Attorney-Client Privilege: Never knowingly listen to or record a conversation between a subject and his or her attorney when other parties are not present. Any time that an attorney is a party to a conversation, call the case agent immediately. If it is determined that a conversation involving an attorney constitutes legal consultation of any kind, notify the case agent, shut off the monitor and stop recording, unless you are able to determine from the interception of any conversation involving an attorney that third parties who are not involved in the legal matters being discussed are present. If such third parties are present, and only if they are present, may you intercept such conversations following the above-described rules of minimization. In any event, notify the case agent immediately.

(b) Parishioner-Clergyman Privilege: All conversations and conduct between a parishioner and his clergyman are to be considered privileged. An electronic surveillance order could not be obtained to listen to a subject confess his sins to a priest in a confessional booth; similarly, a subject discussing his personal, financial or legal problems with his priest, minister, rabbi, etc. may likewise not be intercepted. Thus, if it is determined that a clergyman is a party to a communication being intercepted and that the communication is penitential in nature, turn off the monitor, stop recording, and notify the case agent.

© Doctor-Patient Privilege: Any conversation a patient has with a doctor relating to diagnosis, symptoms, treatment, or any other aspects of physical, mental or emotional health, is privileged. If it is determined that a person is talking to his

doctor and that the conversation concerns the person's health (or someone else's health), turn off the machine and notify the case agent.

(d) Husband-Wife Privilege: As a general rule, there is also a privilege covering communications between lawfully married spouses. Monitoring should be discontinued and the case agent notified if it is determined that a conversation solely between a husband and wife is being intercepted. If a third person is present, however, the communication is not privileged and that conversation may be monitored in accordance with the previously described rules of minimization. If the conversation is between the named subjects and their respective spouses, the conversation may be monitored in accordance with the previously described rules of minimization regarding monitoring these individuals' conversations to determine whether they are discussing crimes. If the nature of the conversation is criminal, monitoring may continue; otherwise, it may not be monitored.

8. Abstracts or summaries of each conversation are to be made at the time of interception and are to be included in the logs and the statistical analysis sheet. If the conversation is not recorded entirely, an appropriate notation should be made indicating the incomplete nature of the conversation and why the conversation was not recorded completely (e.g., "non-pertinent" or "privileged").

9. The logs should reflect all activity occurring at the monitoring station concerning both the intercepted conversations as well as the equipment itself (e.g., "replaced tape," "malfunction of tape recorder," "no overheard conversation"). These logs will be used ultimately to explain the monitoring agent's actions when intercepting communications. It is important to describe the parties to each conversation, the nature of each conversation, and the action taken. All monitoring agents will record the times their equipment is turned on and off.

10. All conversations that are monitored must be recorded.

11. The Log

The monitoring agents should maintain a contemporaneous log, by shifts, of all communications intercepted, indicating the reel and footage locations of each communication; the time and duration of the interception; whether outgoing or incoming in the case of telephone conversations; the number called if the call was outgoing; the participants, if known; and the subjects and a summary of the content of pertinent conversations. Any peculiarities, such as codes, foreign language used, or

background sounds, should also be noted. When the interception of a communication is terminated for purposes of minimization, that fact should be noted. This log should record the names of the personnel in each shift and the function performed by each, malfunctions of the equipment or interruptions in the surveillance for any other reason and the time spans thereof, and interceptions of possibly privileged conversations or conversations relating to crimes not specified in the original interception order. Each entry in the log should be initialed by the person making it.

12. Protection of the Recording

The following procedure should be followed during the period of authorized interceptions:

(a) Either during or at the end of each recording period, copies of the recorded conversations should be made for the use of the investigative agencies and the supervising attorney;

(b) The original recording should be placed in a sealed evidence envelope and kept in the custody of the investigative agencies until it is made available to the court at the expiration of the period of the order; and

© A chain of custody form should accompany the original recording. On this form should be a brief statement, signed by the agent supervising the interception, which identifies:

I - the order that authorized the recorded interceptions (by number if possible);

ii - the date and time period of the recorded conversations;

iii - the identity (when possible) of the individuals whose conversations were recorded; and

iv - the place (e.g., location of telephone) where intercepted communications took place.

(d) The form should indicate to whom the case agent has transferred the custody of the original recording and the date and time that this occurred. Each subsequent transfer, including that to the court, should be noted on the form.

(e) The case agent should mark a label attached to the original tape reel/cassette in order to identify it as corresponding with accompanying chain of custody forms. The

date of the recording should also be marked on the label and this should be initialed by the agent.

(f) Each agent or other person signing the chain of custody form should be prepared to testify in court that the original tape, while in his custody, was kept secure from the access of third parties (unless noted to the contrary on the form) and was not altered or edited in any manner. It is the responsibility of the investigative agencies to ensure that original recordings in their custody will be maintained in such a way as to ensure their admissibility in evidence at trial over objections to the integrity of the recording.

13. Procedure When No Recording Can be Made

In those unusual instances when no recording of the intercepted conversations can be made, the following procedure should be used:

(a) The monitoring agent should make a contemporaneous log or memorandum that is as near to a verbatim transcript as is possible;

(b) The log or memorandum should close with a brief statement signed by the agent indicating the date, time, and place of the intercepted conversation. The order authorizing the interception should be identified. The agent should indicate that the log or memorandum contains the contents of the intercepted communication which he overheard. This should be followed by the agent's signature; and

© This log should be treated by the investigative agencies as if it were an original recording of the intercepted communication.

14. If the conversation occurs in a language other than English that no one at the monitoring post understands, the entire conversation should be monitored and recorded and then minimized by a person familiar with the investigation, but who is not actively involved in it, in accordance with the minimization rules set forth above.

15. If anything appears to be breaking suddenly, please call the case agent or the AUSA. Several telephone numbers will be posted at the monitoring post.

_____

Assistant United States Attorney

Application for Electronic Communications Interception

UNITED STATES DISTRICT COURT
_____ DISTRICT OF _____

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER AUTHORIZING THE INTERCEPTION OF ELECTRONIC COMMUNICATIONS	)

APPLICATION FOR INTERCEPTION OF ELECTRONIC COMMUNICATIONS

_____, Assistant United States Attorney, _____ District of _____/Special Attorney, United States Department of Justice, being duly sworn, states:

1. I am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code, that is, an attorney authorized by law to prosecute or participate in the prosecution of United States federal felony offenses. I am also an attorney for the Government as defined in Rule 1(b)(1) of the Federal Rules of Criminal Procedure, and, therefore, pursuant to Section 2516(3) of Title 18, United States Code, I am authorized to make an application to a Federal judge of competent jurisdiction for an order authorizing the interception of electronic communications.

2. This application is for an order pursuant to Section 2518 of Title 18, United States Code, authorizing the interception of electronic communications for a thirty (30) day period of (name the interceptees) and others as yet unknown to (and from) the (telephone/digital-display paging device(s)/facsimile machine/computer/internet account number _____) (bearing or using the telephone number(s) _____, subscribed to by _____) concerning federal felony offenses, that is, offenses involving violations of (list the section(s) of the United States Code and briefly describe the applicable offense(s)).

3. I have discussed all of the circumstances of the above offenses with Special Agent _____ of the _____, who has directed and conducted this investigation, and have examined the Affidavit of Special Agent _____ of this date (attached to this application as

Exhibit __, and which is incorporated by reference). Whereof your applicant states upon information and belief that:

a. there is probable cause to believe that (name the violators) have committed, are committing and will continue to commit violations of (list the offenses);

b. there is probable cause to believe that particular electronic communications of (name the interceptee(s)) concerning the above-described offenses will be obtained through the interception for which authorization is herein applied. In particular, there is probable cause to believe that the communications to be intercepted will concern the telephone numbers of associates of (name the violators) and the dates, times and places for commission of the aforementioned federal felony offenses when (name the interceptees) communicate with their co-conspirators, aiders and abettors, and other participants in the conspiracy, thereby identifying the co-conspirators and aiders and abettors of (name the violators) and others as yet unknown, their places of operation. In addition, these communications are expected to constitute admissible evidence of the above-described offenses;

c. normal investigative procedures have been tried and have failed, reasonably appear to be unlikely to succeed if tried, or are too dangerous to employ, as are described in further detail in the attached affidavit of Special Agent _____; and

d. there is probable cause to believe that (list the facilities from which, or the place where, the electronic communications are to be intercepted) are being, and will continue to be used in connection with the commission of the above-described offenses.

The attached affidavit contains a full and complete statement of facts concerning all previous applications that have been made to any judge of competent jurisdiction for authorization to intercept, or for approval of interception of wire, oral or electronic communications involving any of the same individuals, facilities, or places specified in this application.

On the basis of the allegations contained in this application and on the basis of the attached affidavit of Special Agent _____,

IT IS HEREBY REQUESTED that this Court issue an order, pursuant to the power conferred on it by Section 2518 of Title

18, United States Code, authorizing the (name the investigative agency/agencies) to intercept electronic communications to (and from) the above-described (telephone/digital display paging device, facsimile machine, computer, internet account), and providing that such interceptions not terminate automatically after the first interception that reveals the manner in which the alleged co-conspirators and others as yet unknown conduct their illegal activities, but continue until all communications are intercepted which reveal fully the manner in which the above-named persons and others as yet unknown are committing the offenses described herein, and which reveal fully the identities of their confederates, their places of operation, and the nature of the conspiracy involved therein, or for a period of thirty (30) days measured from the day on which investigative or law enforcement officers first begin to conduct an interception under this Court's order or ten (10) days after this order is entered, whichever is earlier.

IT IS REQUESTED FURTHER that in the event that the target facility is transferred outside the territorial jurisdiction of this Court, interceptions may take place in any other jurisdiction within the United States.

IT IS REQUESTED FURTHER that this Court issue an order pursuant to Section 2518(4) of Title 18, United States Code, directing that (list the communications service provider(s)), a communication service provider as defined in Section 2510(15) of Title 18, United States Code, shall furnish, and continue to furnish, the applicant and investigative agency with all information, facilities and technical assistance necessary to accomplish the interceptions unobtrusively and with a minimum of interference with the services that such providers are according the persons whose communications are to be intercepted, and to ensure an effective and secure installation of electronic devices capable of interception of electronic communications to (and from) the above-described (telephone/digital display paging device/facsimile machine/computer/internet account), with the service provider to be compensated by the applicant for reasonable expenses incurred in providing such facilities or assistance.

IT IS REQUESTED FURTHER that, to avoid prejudice to this criminal investigation, the Court order the said providers of electronic communication service and their agents and employees not to disclose or cause a disclosure of this Court's order or the request for information, facilities and assistance by the (identify the investigative agency/agencies) or the existence of the investigation to any person other than those of their agents and employees who require said information to accomplish the services hereby requested. In particular, said providers and

their agents and employees should be ordered not to make such disclosure to a lessee, telephone subscriber, or any interceptee or participant in the intercepted communications.

IT IS REQUESTED FURTHER that this Court direct that this order be executed as soon as practicable after it is signed and that all monitoring of communications shall be recorded and examined by monitoring agents or attorneys to determine the relevance of the intercepted electronic communications to the pending investigation and that the disclosure of the contents or nature of the electronic communications intercepted be limited to those communications relevant to the pending investigation, in accordance with the minimization requirements of Chapter 119 of Title 18, United States Code. The interception of communications authorized by this Court's order must terminate upon attainment of the authorized objectives or, in any event, at the end of thirty (30) days measured from the earlier of the day on which investigative or law enforcement officers first begin to conduct an interception under this Court's order or ten (10) days after the order is entered, whichever is earlier.

IT IS REQUESTED FURTHER that the Court order that either Assistant United States Attorney/Special Attorney _____, or any other Assistant United States Attorney/Special Attorney familiar with the facts of this case, provide to the Court a report on or about the (tenth), (twentieth) and (thirtieth) days following the date of this order showing what progress has been made toward achievement of the authorized objectives and the need for continued interception. If any of the aforementioned reports should become due on a weekend or holiday, IT IS REQUESTED FURTHER that such report become due on the next business day thereafter.

IT IS REQUESTED FURTHER that the Court order that its orders, this application and the accompanying affidavit and proposed order(s), and all interim reports filed with the Court with regard to this matter be sealed until further order of this Court, except that copies of the order(s), in full or redacted form, may be served on the (identify the investigative agency/agencies) and the service provider(s) as necessary to effectuate the Court's order as set forth in the proposed order(s) accompanying this application.

DATED this _____ day of _____, 20__.

_____

Assistant United States Attorney

SUBSCRIBED and SWORN to before me
this _____ day of _____, 20__.

_____
UNITED STATES DISTRICT COURT JUDGE
(District)

Affidavit for Electronic Communications Interception

UNITED STATES DISTRICT COURT
_____ DISTRICT OF _____

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER AUTHORIZING THE INTERCEPTION OF ELECTRONIC COMMUNICATIONS	MISC. NO.

AFFIDAVIT IN SUPPORT OF APPLICATION

_____, being duly sworn, deposes and states as follows:

1. I am a Special Agent with the _____, United States Department of Justice. I have been so employed by the _____ for the past _____ ( ) years. I have participated in investigations involving (organized crime/drug trafficking, etc.) activities for the past _____ ( ) years.

(Describe present assignment)

2. I am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code, in that I am empowered by law to conduct investigations and to make arrests for federal felony offenses.

3. This affidavit is submitted in support of an application for an order authorizing the interception of electronic communications occurring (specify the facility or facilities to which the application and affidavit are directed).

4. I have participated in the investigation of the above offenses. As a result of my personal participation in this investigation, through interviews with and analysis of reports submitted by other (Special Agents of the _____ and/or other state/local law enforcement personnel), and by the analysis of (surveillance logs/pen register information, etc.), I am familiar with all aspects of this investigation. On the basis of this familiarity, and on the basis of other information which I have reviewed and determined to be reliable, I allege that:

a. there is probable cause to believe that (list the violators) have committed, are committing, and will continue

to commit (list the offense(s) - can be any federal felony offense).

b. there is probable cause to believe that particular electronic communications of (list the interceptees) concerning the above offenses will be obtained through the interception of such communications to (and from)the (telephone/digital pager/facsimile machine/computer/internet account) (assigned/using/bearing account/telephone number(s) _____, subscribed to by _____, (and, if applicable, the facility's physical location)). In particular, there is probable cause to believe that the communications to be intercepted will concern the (telephone numbers of associates of (list the violator(s)) and the dates, times, places, and plans for commission of the aforementioned federal felony offenses when (list the interceptees) communicate with their co-conspirators, aiders and abettors, and other participants in the conspiracy, thereby identifying the co-conspirators and aiders and abettors of (the violators), and others as yet unknown, their places of operation, (etc.). In addition, these communications are expected to constitute admissible evidence of the above-described offenses.

c. normal investigative procedures have been tried and have failed, reasonably appear to be unlikely to succeed if tried, or are too dangerous to employ, as is described herein in further detail.

d. there is probable cause to believe that (list the facilities over which the electronic communications are to be intercepted) are being, and will continue to be, used in connection with the commission of the above offenses.

PERSONS EXPECTED TO BE INTERCEPTED

Include a short description of each expected interceptee; if appropriate, explain why certain participants in the offenses are not expected to be interceptees.

FACTS AND CIRCUMSTANCES

Provide an in-depth discussion of the facts in support of the probable cause statements above. If informant information provides a basis for any of the probable cause for any of the required information, provide adequate qualifying language for each informant.

(In drug cases, if appropriate, include a "facts and circumstances" paragraph regarding use of pagers, e.g., "I know

from my training, experience, and discussions with other experienced agents that narcotics traffickers frequently use paging devices to further their illicit business. Pagers permit co-conspirators to contact each other with virtually no possibility that their communications will be intercepted. For example, the type of paging device used in this matter allows a conspirator to signal a confederate, identify himself through a numerical code, and convey the number of a secure or non-suspect telephone, usually a pay telephone, at which he can be contacted. The conspirator receiving this information can then go to a secure or non-suspect telephone, return the call, and engage in a criminal discussion with his confederate which, under normal circumstances, will be incapable of interception by law enforcement authorities.")

NORMAL INVESTIGATIVE PROCEDURES

Need for Electronic Interception

Based upon your affiant's training and experience, as well as the experience of other (list the Special Agents of the _____ and/or state/local officers of _____), and based upon all of the facts set forth herein, it is your affiant's belief that the interception of electronic communications is the only available technique with a reasonable likelihood of securing the evidence necessary to prove beyond a reasonable doubt that (list the violator(s)), and others as yet unknown are engaged in the above-described offenses.

Numerous investigative procedures that are usually employed in the investigation of this type of criminal case have been tried and have failed, reasonably appear to be unlikely to succeed if they are tried, or are too dangerous to employ.

(Include a discussion of the details of specific problems regarding the use of alternative investigative techniques in this investigation. Then discuss the standard problem areas, as synopsized below, modifying the statements to comport with the actual circumstances of your case.)

Physical Surveillance

Physical surveillance has been attempted on many occasions in this investigation. Although it has proven valuable in identifying some of the targets' activities and associates, physical surveillance, if not used in conjunction with other techniques, including electronic surveillance, is of limited value. Even if highly successful, physical surveillance does not always succeed in gathering evidence of the criminal activity under investigation. It is an investigative technique used to

confirm meetings between alleged conspirators, and usually only leads investigators to speculate as to the purpose of the meeting(s). It is also a technique used to corroborate information obtained from confidential informants. Further, physical surveillance of the alleged conspirators will not establish conclusively the elements of the subjects' violations and has not and most likely will not establish conclusively the identities of various conspirators. Prolonged or regular physical surveillance of the targets would most likely be noticed, causing them to become more cautious in their illegal activities, to flee to avoid further investigation and prosecution, to cause a threat to the safety of the informant(s) and undercover agent(s), or otherwise to compromise the investigation.

With regard to this investigation, physical surveillance is unlikely to establish conclusively the roles of the named conspirators, to identify additional conspirators, to identify the conspirators' sources of supply, or otherwise to provide admissible evidence in regard to this investigation because (provide details of any of the following, as applicable):

- conspirators are using counter-surveillance, such as erratic driving behavior in order to detect surveillance; or have evinced that they suspect law enforcement surveillance of their activities;

- the nature of the neighborhood forecloses physical surveillance (e.g., a close-knit community; cul-de-sac, dead end, or large apartment building; and/or the neighbors all know each other and call the police when surveillance is spotted);

- further surveillance would only serve to alert the conspirators of the law enforcement interest in their activities and compromise the investigation.

Use of Grand Jury Subpoenas

Based upon your affiant's experience and conversations with Assistant United States Attorneys for the _____ District of _____ who have experience prosecuting violations of criminal law, your affiant believes that subpoenaing persons who are believed to be involved in this conspiracy, or their associates before a Federal Grand Jury would most likely not be completely successful in achieving the stated goals of this investigation. The targets of this investigation, and their co-conspirators and other participants, should they be called to testify before the Grand Jury, would most likely be uncooperative and invoke their Fifth Amendment privilege not to testify. It

would then be unwise to seek any kind of immunity for any of these persons because the granting of such immunity might foreclose prosecution of the most culpable members of this conspiracy, and could not ensure that such immunized witnesses would provide truthful testimony before the Grand Jury. Additionally, the service of Grand Jury subpoenas upon the targets or their co-conspirators would only alert the targets to the existence of this investigation, thereby causing them to become more cautious in their activities, to flee to avoid further investigation or prosecution, to threaten the lives of the informant(s) and the undercover agent(s), or otherwise to compromise this investigation.

(Add specific information about any persons who have been subpoenaed before the Grand Jury, especially when the Fifth Amendment was invoked or when the witness later advised the targets.)

Confidential Informants and Cooperating Sources

Reliable confidential informants/cooperating sources have been developed and used, and will continue to be developed and used, in regard to this investigation, but these sources (discuss those that are applicable):

- exist on the fringe of this organization and, therefore, have no direct contact with mid- or high-level members of the organization; or such contact is virtually impossible because the sources have no need to communicate with such individuals;

- refuse to testify before the Grand Jury or at trial because of a fear for personal or family safety; or their testimony would be uncorroborated or otherwise subject to impeachment (due to prior record, criminal involvement, etc.);

- are no longer associated with the targets of this investigation and their information is included for historical purposes only.

None of the confidential informants described in this affidavit are able to furnish information that would identify fully all members of this ongoing criminal conspiracy or define the roles of those conspirators sufficiently for prosecution or that would identify sufficiently (the source(s) of supply or all details of delivery, quantities, financial arrangements, and the like), etc.

Your affiant believes that information provided by the confidential sources, even if all sources agreed to testify, would not, without the evidence available through the requested electronic surveillance, result in a successful prosecution of all of the participants.

Undercover Police Officers and Agents

Undercover police officers and/or agents have been unable to infiltrate the inner workings of this conspiracy due to the close and secretive nature of this organization. Your affiant believes that there are no undercover officers/agents who can infiltrate the conspiracy at a level high enough to identify all members of the conspiracy or otherwise satisfy all the goals of this investigation. (Indicate if infiltration is not feasible because the confidential informant(s) is not in a position to make introductions of undercover officers to mid- or high-level members of the organization.)

(Details of the use of undercover officers should have been provided in the body of this affidavit, with this section indicating the limitations of such usage.)

Interviews of Subjects or Associates

Based upon your affiant's experience, your affiant believes that interviews of subjects or their known associates would produce insufficient information concerning the identities of all of the persons involved in the conspiracy, the source of the drugs, financing, etc., the location of records, drugs, etc., or other pertinent information regarding the subject crimes. Your affiant also believes that any responses to the interviews would contain a significant number of half-truths and untruths, diverting the investigation with false leads or otherwise frustrating the investigation. Additionally, such interviews would likely result in non-targeted interviewees alerting the members of the conspiracy, thereby compromising the investigation and resulting in the possible destruction or concealment of (documents) (other evidence) and the possibility of harm to cooperating source(s), the identity of whom may become known or whose existence may otherwise be compromised.

(This portion of the affidavit is sometimes merged with the discussion regarding the use of the Federal Grand Jury. Any actual interviews conducted, and any resulting problems should also be discussed here.)

Search Warrants

The execution of search warrants in this matter has been considered. However, use of such warrants would, in all likelihood, not yield a considerable quantity of narcotics or relevant documents, nor would the searches conducted pursuant to such warrants be likely to reveal the total scope of the criminal operation and the identities of the co-conspirators. (It is unlikely that all, or even many, of the principals of this organization would be at any one location when a search warrant was executed.) Your affiant believes that search warrants executed at this time would be more likely to compromise the investigation by alerting the principals of the investigation, thereby, allowing unidentified co-conspirators to insulate themselves further from successful detection, as well as to otherwise frustrate the purposes of this investigation. (If search warrants were executed, then discuss the results and why this information is not enough to satisfy the goals of the investigation.)

Pen Registers/Telephone Tolls/Trap and Trace

Telephone toll/pen register/trap and trace information has been used in this investigation, as described above. (Provide a synopsis of the results obtained from a review of these phone records; describe why this information is insufficient to identify fully other coconspirators or fulfill the needs of the investigation.)

Other Limitations

(Provide details as to violence (murdered or hurt witnesses, threats, etc.) and other situations present in this investigation that limit the effectiveness of normal investigative techniques.)

Based upon the foregoing, it is your affiant's belief that the interception of electronic communications is an essential investigative means in obtaining evidence of the totality of the offenses in which the subject(s) and others as yet unknown are involved.

PRIOR APPLICATIONS

Based upon a check of the records of the Federal Bureau of Investigation, (and any other pertinent agency) no prior applications for an order authorizing the interception of wire, oral or electronic communications have been made involving the persons, premises or facilities named herein. If the facts warrant, include additional information concerning prior or ongoing electronic surveillance, (person named, court that issued

the order, date and relevance, if any, to the current investigation.)

MINIMIZATION

Suggested language for pagers:

All monitoring of electronic communications to (and from) the (telephone/digital-display paging device/facsimile machine/computer/internet account) assigned number ( ) _____, will be recorded and examined by monitoring agents and attorneys to determine their relevance to the pending investigation. The disclosure of the contents or nature of the electronic communications intercepted will be limited to those communications relevant to the pending investigation, in accordance with the minimization requirements of Chapter 119 of Title 18, United States Code.

Suggested language for facsimile machines:

All interceptions will be minimized in accordance with Chapter 119 of Title 18, United States Code. Fax transmissions sent or received by _____ will be minimized as follows: each fax transmission will be printed on the machine used to intercept fax communications. The monitoring agent and AUSA will decide, based on the identities of the sender and recipient and the subject matter of the transmission, whether the fax appears to be pertinent to the criminal offenses listed in the court's order. If the fax does not appear to be pertinent, the intercepted transmission will be placed in an envelope and sealed. It will then be placed in a locked drawer until it is turned over to the court with the other intercepted transmissions after the interception order has expired. (If the facsimile machine is a dedicated to fax transmissions only or, if the facsimile machine is attached to a telephone, but the government has not applied for authorization to intercept wire communications over the telephone, then add: "It is not the intention of the Government to intercept wire communications during this investigation; only electronic communications will be intercepted.")

Because of the type of information intercepted, i.e., typewritten fax communications and not verbal communications, the monitors will be unable to minimize any non-pertinent information until after it has been received at the monitoring location. It is anticipated that the monitoring location will not be staffed at all times, but will be activated electronically. The monitoring location will be kept secure and access will be

available only to persons authorized to be involved with this investigation.

CONCLUSION

Your affiant believes that the facts alleged herein establish that the targets of this investigation are engaged in an ongoing criminal enterprise and that the evidence sought will be intercepted on a continuing basis following the first receipt of the particular communications that are the object of this request. Therefore, it is requested that the interception not be required to terminate when the communications described herein are first intercepted, but be allowed to continue until communications are intercepted which fully reveal the scope of the enterprise, including the identities of all participants, their places and methods of operation, and the various criminal activities in which they are engaged which are in furtherance of the enterprise, not to exceed thirty (30) days measured from the earlier of the day on which investigative or law enforcement officers first begin to conduct an interception under this Court's Order or ten (10) days after the Order is entered.

_____
(NAME)
Special Agent
(Agency)

Sworn to before me this
_____ day of _____, 20_.

_____
UNITED STATES DISTRICT COURT JUDGE
(District)

Order for Interception of Electronic Communications

UNITED STATES DISTRICT COURT
_____ DISTRICT OF _____

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER AUTHORIZING THE INTERCEPTION OF ELECTRONIC COMMUNICATIONS	)

ORDER AUTHORIZING THE INTERCEPTION OF
ELECTRONIC COMMUNICATIONS

Application under oath having been made before me by _____, Assistant United States Attorney, _____ District of _____/Special Attorney, United States Department of Justice, an "investigative or law enforcement officer" of the United States within the meaning of Section 2510(7) of Title 18, United States Code, and an attorney for the Government as defined in Rule 1(b)(1) of the Federal Rules of Criminal Procedure, for an Order authorizing the interception of electronic communications pursuant to Section 2518 of Title 18, United States Code, and full consideration having been given to the matter set forth therein, the Court finds:

a. there is probable cause to believe that (list the violators) have committed, are committing, and will continue to commit violations of (list the offenses - can be any federal felony offense);

b. there is probable cause to believe that particular electronic communications of (list the interceptees) concerning the above-described offenses will be obtained through the interception for which authorization is herein applied. In particular, there is probable cause to believe that the communications to be intercepted will concern the telephone numbers of associates of (the violator(s)) and the dates, times, places and plans for commission of the aforementioned federal felony offenses when (list the interceptee(s)) communicate with their co-conspirators, aiders and abettors and other participants in the conspiracy, thereby identifying the co-conspirators and others as yet unknown, their places of operation, (etc.). In addition, these communications are expected to constitute admissible evidence of the above-described offenses;

c. It has been established adequately that normal investigative procedures have been tried and have failed, reasonably appear to be unlikely to succeed if tried, or are too dangerous to employ;

d. there is probable cause to believe that (list the facilities over which the electronic communications are to be intercepted) have been, are being and will continue to be used in connection with the commission of the above-described offenses.

WHEREFORE, IT IS HEREBY ORDERED that Special Agents of the (name the investigative agency/agencies) are authorized to intercept electronic communications over the above-described facilities.

PROVIDED that such interception(s) shall not terminate automatically after the first interception that reveals the manner in which the alleged co-conspirators and others as yet unknown conduct their illegal activities, but may continue until all communications are intercepted which fully reveal the manner in which the above-named persons and others as yet unknown are committing the offenses described herein, and which reveal fully the identities of their confederates, their places of operation, and the nature of the conspiracy involved therein, or for a period of thirty (30) days measured from the day on which investigative or law enforcement officers first begin to conduct an interception under this Order or ten (10) days after this Order is entered, whichever is earlier.

IT IS ORDERED FURTHER that, pursuant to 18 U.S.C. § 2518(3), in the event that the target facility is transferred outside the territorial jurisdiction of this court, interceptions may take place in any other jurisdiction within the United States.

IT IS ORDERED FURTHER that, based upon the request of the Applicant pursuant to Section 2518(4) of Title 18, United States Code, (name the communication service provider(s)), communication service provider(s) as defined in Section 2510(15) of Title 18, United States Code, shall furnish, and continue to furnish, the Applicant and the investigative agency/agencies with all information, facilities, and technical assistance necessary to accomplish the interceptions unobtrusively and with a minimum of interference with the services that such provider(s) is according the persons whose communications are to be intercepted, with the service provider(s) to be compensated by the Applicant for reasonable expenses incurred in providing such facilities or assistance.

IT IS ORDERED FURTHER that, to avoid prejudice to the Government's criminal investigation, the above provider(s) of

electronic communication service and its agents and employees are ordered not to disclose or cause a disclosure of this Order or the request for information, facilities, and assistance by the (name the investigative agency/agencies) or the existence of the investigation to any person other than those of its agents and employees who require said information to accomplish the services hereby ordered. In particular, said provider(s) and its agents and employees shall not make such disclosure to a lessee, telephone or paging device subscriber or any interceptee or participant in the intercepted communications.

IT IS ORDERED FURTHER that this Order shall be executed as soon as practicable and that all monitoring of the electronic communications shall be recorded and examined by the monitoring agents or attorneys to determine the relevance of the intercepted electronic communications to the pending investigation and that the disclosure of the contents or nature of the electronic communications intercepted be limited to those communications relevant to the pending investigation, in accordance with the minimization requirements of Chapter 119 of Title 18, United States Code. The interception of communications must terminate upon the attainment of the authorized objectives, not to exceed thirty (30) days measured from the earlier of the day on which investigative or law enforcement officers first begin to conduct an interception under this Order or ten (10) days after the Order is entered.

IT IS ORDERED FURTHER that Assistant United States Attorney/Special Attorney _____ or any other Assistant United States Attorney/Special Attorney familiar with the facts of this case shall provide this Court with a report on or about the (tenth), (twentieth) and (thirtieth) days following the date of this Order showing what progress has been made toward achievement of the authorized objectives and the need for continued interception. If any of the above-ordered reports should become due on a weekend or holiday, IT IS ORDERED FURTHER that such report shall become due on the next business day thereafter.

IT IS ORDERED FURTHER that this Order, the application, affidavit, and proposed Order(s), and all interim reports filed with this Court with regard to this matter shall be sealed until further order of this Court, except that copies of the Order(s), in full or redacted form, may be served on the (investigative agency/agencies) and the service provider(s) as necessary to effectuate this Order.

_____
UNITED STATES DISTRICT COURT JUDGE
(District)

DATED this _____ day of _____, 20__.

Sample Title III Roving Affidavit

Written by:

Julie Wuslich
Chief, Electronic Surveillance Unit
Office of Enforcement Operations
United States Department of Justice
Criminal Division
(202) 514-6809

Jeffery S. Spalding
Deputy Chief, Electronic Surveillance Unit
Office of Enforcement Operations
United States Department of Justice
Criminal Division
(202) 514-6809

May 2005

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF MICHIGAN
GRAND RAPIDS DIVISION

IN THE MATTER OF THE APPLICATION	*	
OF THE UNITED STATES OF AMERICA	*	
FOR AN ORDER AUTHORIZING THE	*	MISC. NO.
INTERCEPTION OF WIRE COMMUNICATIONS	*	
OCCURRING TO AND FROM THE CELLULAR	*	UNDER SEAL
TELEPHONES BEARING THE NUMBERS	*	
(616) 555-6068, and accessed through	*	
IMSI 316000115672568 AND (616) 555-6015	*	
and assigned ESN 345678000; AND THE	*	
ROVING INTERCEPTION OF WIRE	*	
COMMUNICATIONS OVER **VARIOUS**	*	
AND CHANGING CELLULAR TELEPHONES	*	
USED BY JACOB RIPLEY	*	

AFFIDAVIT IN SUPPORT OF APPLICATION[8]

I. INTRODUCTION

I, J. Kenneth Smith, a Special Agent with the Drug Enforcement Administration ("DEA")[9], being duly sworn, state as follows:

1. I am a Special Agent with the DEA, duly appointed according to the law and acting as such, and have been employed by the DEA since February 1993. As a DEA Special Agent, I am an "investigative or law enforcement officer" within the meaning of Title 18, United States Code, Section 2510(7), that is, an officer of the United States who is empowered by law to conduct

[8] This sample roving affidavit pertains to a fictitious narcotics trafficking investigation and should be consulted when drafting Title III roving pleadings. When using this affidavit as a reference, assume that it was submitted for authorization to the Office of Enforcement Operations ("OEO") in mid-December 2004, taking note that the information in support of probable cause is up-to-date. Specific questions regarding all Title III issues should be addressed to OEO at (202) 514-6809.

[9] Department of Justice ("the Department") policy precludes the use of multiple affiants except when it is indicated clearly which affiant swears to which part of the affidavit, or that each affiant swears to the entire affidavit. For practical purposes, a single affiant should be used.

investigations and to make arrests for offenses enumerated in Title 18, United States Code, Section 2516.[10]

2. I am currently assigned to the DEA Grand Rapids Field Office. In connection with my official duties as a Special Agent of the DEA, I am responsible for conducting investigations into violations of Title 21 of the United States Code and other federal criminal statutes. During my twelve (12) years as a DEA Special Agent, I have participated in numerous narcotics investigations, including more than fifty (50) investigations in which I have been designated as the lead investigative agent. These investigations have resulted in the arrest of more than seventy (70) persons and the seizure of marijuana, methamphetamine, cocaine, MDMA, heroin, and other controlled substances. During the course of these investigations, I have conducted or participated in physical and electronic surveillance; prepared affidavits which have resulted in court ordered wire interceptions; applied for, obtained, and executed more than thirty federal search warrants; conducted numerous debriefings of informants, cooperating defendants, and other individuals cooperating with the United States; seized and evaluated items of evidence; and reviewed taped conversations, seized narcotics records, and financial documents.

3. This affidavit is submitted in support of an application for an order authorizing the interception of wire communications[11] occurring to and from the prepaid cellular telephone bearing the number (616) 555-6068, subscribed to by Janis Jenkins, 1555 N. Shore Rd., Grand Haven, Michigan[12], and

---

[10] If a state or local law enforcement officer is the affiant for a federal electronic surveillance affidavit, he/she must be deputized as a federal officer of the agency with responsibility for the offenses under investigation. See, 18 U.S.C. § 2516(1) (interceptions are to be conducted by the federal agency responsible for the offenses for which the application is made); United States v. Lyons, 695 F.2d 802 (4th Cir. 1982).

[11] Cellular telephones often are equipped with features allowing the transmission of both wire (voice over the phone) and electronic (e.g., text-messages and/or email) communications. Under current Department policy, a separate showing of probable cause for each type of communication sought to be intercepted is needed to obtain Department authorization to apply for a court order to intercept each type of communication. This policy is based on the explicit wording of the Title III statute, as well as the legislative history of Title III. See, 18 U.S.C. § 2518(1)(b) (requiring a particular description of the type of communications sought to be intercepted in each application for an order authorizing or approving the interception of wire, oral, or electronic communications), § 2518(3)(b) (requiring facts showing probable cause to believe that particular communications concerning that offense will be intercepted), and § 2518 (requiring that the order specify the particular type of communications to be intercepted and a statement of the particular offense to which it relates)..

[12] When identifying the targeted telephone(s), the telephone number(s) and subscriber address(es) (as it appears in service provider records) should be included. In some instances, no subscriber

accessed through international mobile subscriber identification ("IMSI") number 316000115672568[13] (**"Target Phone 1"**) and the cellular telephone bearing the number (616) 555-6015, subscribed to by Steven Hill, 512 S. Division Street, Grand Rapids, Michigan, and assigned electronic serial number ("ESN")[14] 345678000 (**"Target Phone 2"**); As discussed below, **Target Phones 1 and 2** are used by Jacob Ripley ("Ripley").[15] Additionally, this affidavit is submitted in support of an application that seeks authorization, pursuant to Title 18, United States Code, Section 2518(11)(b)[16], to intercept the wire communications

---

information will be available, most often in the case of prepaid cellular telephones.

[13] An IMSI number is a fifteen (15) digit number assigned to a removable computer chip located inside certain service providers' cellular telephones. IMSI numbers are unique to each individual subscriber, and the chip on which the IMSI number is encoded can be removed and used in other similarly-equipped telephones. Depending on the service provider, these numbers are labeled international mobile subscriber "identification/identifier/identity" numbers.

[14] An ESN is a serial number embedded in a particular telephone instrument. The ESN number is permanently assigned to that particular piece of telephone hardware, is unique to that facility, and cannot be changed without obtaining a new telephone. New telephone numbers can be assigned to an ESN.

[15] When seeking authorization to intercept roving wire communications of a particular target, the current cellular telephone(s) being used by the roving target at the time of the application should be specifically targeted in the application and order. Specifically targeting a phone in the application and order allows law enforcement to continue tapping that telephone should the roving target hand it off to a co-conspirator. Phones that are not specifically targeted in the pleadings cannot be monitored if the roving target hands off the telephone to someone else, even if that person is going to use the telephone to facilitate criminal activities. Remember, roving authority is person-specific.

This process is repeated in any subsequent extensions and/or spinoffs of the roving wiretap, with new phones in the hands of the roving target at the time of the extension/spinoff specifically identified and targeted, along with an extension of the roving authority, as the facts warrant. It is important to note that a regular Title III authorization is specific to particular telephones (i.e., interceptions can continue no matter who is using that facility as long as the telephone is being used to facilitate predicate Title III offenses). Conversely, a roving Title III authorization is specific to the particular person (i.e., telephones wiretapped pursuant to the roving authorization can only continue as long as *the roving target is using those telephones*). If the roving target stops using one of the "various and changing" cellular telephones (i.e., those phones intercepted during the roving authorization period that were not specifically identified in the original Title III order), interception over those facilities must cease.

[16] The roving provision of Title III is codified in 18 U.S.C. § 2518(11). The roving interception of oral communications (18 U.S.C. § 2518(11)(a)), and wire and electronic communications (18 U.S.C. § 2518(11)(b) are contemplated under the roving statute. Specific citation to 18 U.S.C.(11)(a) and/or (b) should be included be included in the Title III affidavit, depending of the type of communications

occurring to and from **various and changing cellular telephones** used by Ripley during the authorization period.[17]

4. As set forth in greater detail below, Ripley is the leader of a large-scale, Grand-Rapids-based cocaine and heroin distribution organization ("the Grand Rapids Cell") which is a distribution cell of a larger, Mexico-based narcotics organization ("the Ramirez Organization") headed by Roberto Ramirez ("Ramirez"). Confidential source information, court-authorized wire interceptions, physical surveillance, and the analysis of telephone records have established that Ripley directs the distribution of cocaine and heroin in Western Michigan that is transported there from Chicago, Illinois, following its importation from Mexico from the Ramirez Organization, and that Ripley uses the **Target phones 1 and 2** and **various and changing cellular telephones** to facilitate his illegal activities. Specific information related to Ripley's use of **Target Phones 1 and 2 and various and changing cellular telephones** to facilitate his narcotics trafficking activities is set forth below.

5. Ripley has an established pattern of using **various and changing cellular telephones** to accomplish his criminal goals. Ripley changes or "drops" cellular telephones regularly after short periods of time, with the effect of thwarting the ability of law enforcement to conduct electronic surveillance. Investigative facts to date, discussed below, establish that Ripley typically uses a cellular telephone for an average of 18

---

sought to be intercepted.

[17] Generally, to justify a roving wiretap the specifically identified roving target must have dropped three or more telephones in a short period of time. The general Department rule has been that if a criminal subject uses a particular phone for longer than 21 days, a roving wiretap is not appropriate. However, there is flexibility with regard to this 21 day rule when, despite the government's best efforts, the roving target is dropping telephones before effective, regular Title III surveillance can be accomplished. For example, when a subject utilizes multiple cellular telephones in succession for longer than 21 days, but in a manner that makes it difficult to obtain a traditional interception order, a roving wiretap may be authorized.

When a subject's use of multiple phones does not justify a roving wiretap, the solution is often to seek authorization to wiretap all of the identified phones (sometimes referred to as a "block" of cellular telephones) that the subject is using. While a showing of probable cause must still be made as to the use of each of these facilities, this can be accomplished in two steps. First, a showing of independent probable cause as to the use of at least one of the phones to facilitate criminal conversations (e.g. through comments to an informant or undercover agent, or through intercepted calls over another tapped facility). Second, once one phone is clearly established as "dirty," the government can seek authorization as to other facilities where an analysis of telephone records shows a similar calling pattern with that of the phone that has independent probable cause, or where there is other credible information indicating that the subject uses multiple phones that can ultimately be identified.

days before replacing that cellular telephone with another. Based on my training and experience, I know that narcotics traffickers change telephones in this manner in an attempt to avoid detection by law enforcement.

6. I have participated in an ongoing investigation into the Grand Rapids Cell's illegal activities. As a result of my personal participation in this investigation, through interviews with and analysis of reports submitted by other Special Agents of the DEA and other state and local law enforcement personnel, I am familiar with all aspects of this investigation. On the basis of this familiarity, and on the basis of other information which I have reviewed and determined to be reliable, I allege the facts to show that:

a. there is probable cause to believe that Jacob Ripley a/k/a "Jack"; Steven Hass ("Hass"); LeAndra Langdon ("Langdon") a/k/a "Molly"; Christopher Succrattao ("Succrattao"); Robert Gemink ("Gemink") a/k/a "Big Bobby"; Stanley Paul ("Paul"); "Mr. C."; Roberto Ramirez ("Ramirez"); Raul LNU, Regatto LNU, and others as yet unknown (collectively referred to as the "**Target Violators**")[18], are committing, and will continue to commit offenses enumerated in Section 2516 of Title 18 of the United States Code, namely, the importation of cocaine and heroin, the distribution of and possession with intent to distribute cocaine and heroin, and attempts and conspiracies to do the same, all in violation of Title 21, United States Code, Sections 841, 846, 952, 960, and 963; use of wire facilities to facilitate the commission of the above narcotics offenses, in violation of Title 21, United States Code, Section 843; money laundering and conspiracy, in violation of Title 18, United States Code, Sections 1956 and 1957; and aiding and abetting the offenses described above, in violation of Title 18, United States Code, Section 2 (collectively referred as "**the Target Offenses**").[19]

b. there is probable cause to believe that particular wire communications of Ripley, Hass, Langdon, Succrattao, Gemink, Paul, "Mr. C," Raul LNU, Regatto LNU (collectively referred to as

---

[18] If probable cause exists to believe that a person is involved in the criminal offenses under investigation, that person must be named as a target violator (sometimes referred to as "target subject") in the Title III application. Target violators include everyone involved in the criminal conspiracy, even if those individuals are not expected to be intercepted during the Title III authorization period. If the Title III investigation is directed at their activities, they should be named as targets.

[19] The offenses for which you can conduct electronic surveillance are listed in 18 U.S.C. § 2516. Probable cause for at least one Title III predicate must be present in the Title III affidavit. Criminal Division policy requires that non-predicate offenses also be alleged in the Title III application, where probable cause exists for those offenses.

"the **Target Interceptees**")[20] concerning the above offenses will be obtained through the interception of such communications to and from **Target Phones 1 and 2** and, pursuant to Title 18, United States Code, Section 2516(11)(b) the interception of wire communications over **various and changing cellular telephones** used by Ripley.[21]

7. In particular, these communications are expected to concern the specifics of the above offenses, including (I) the nature, extent and methods of the Ramirez Organization's (and Grand Rapids Cell's) narcotics trafficking activities; (ii) the identities and roles of accomplices, aiders and abettors, co-conspirators and participants in their illegal activities; (iii) the distribution and transfer of the contraband and money involved in those activities; (iv) the existence and location of records; (v) the location and source of resources used to finance their illegal activities; (vi) the location and disposition of the proceeds from those activities; and (vii) the locations and items used in furtherance of those activities. In addition, these wire communications are expected to constitute admissible evidence of the commission of the above-described offenses.

8. The statements contained in this affidavit are based in part on information provided by Special Agents of the DEA, on conversations held with detectives and officers from the Michigan State Police ("MSP"), the Grand Rapids Police Department ("GRPD"), on information provided by confidential sources, through court-ordered wire interceptions, and on my experience and background as a Special Agent of the DEA. Since this affidavit is being submitted for the limited purpose of securing authorization for the interception of wire communications, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish the necessary foundation for an order authorizing the interception of wire communications. I have also set forth below my characterization of various coded conversations that have occurred in this investigation among the **Target Violators** and others. My interpretation of these conversations is based on my training and experience, as well my knowledge of the facts of the investigation, including my conversations with confidential sources about the true meaning of the coded conversations.

---

[20] Target interceptees are the violators who are expected to be intercepted over the target phone(s) or the roving phone(s). They are simply a subset of the target violators, and often will include all of the target violators.

[21] As discussed above, the roving authority is person-specific. Law enforcement is permitted to intercept wire communications over various and changing telephones used by the roving target but, unlike a traditional Title III, must cease interceptions over those facilities once the roving target stops using them.

II. PERSONS EXPECTED TO BE INTERCEPTED

9. The following individuals are expected to be intercepted engaging in narcotics-related conversations over **Target Phones 1 and 2 and over various and changing cellular telephones** used by Ripley during the authorization period. The background information on these individuals was obtained from confidential source information (specific information discussed below), court-authorized wire interceptions over cellular telephones in the Southern District of Texas, and a review of court documents:

a. Ripley is a 31 year old male and the leader of the Grand Rapids Cell. Ripley directs the transportation of multi-kilogram quantities of cocaine and heroin from Chicago, Illinois, to the Grand Rapids, Michigan, area, for distribution. Ripley maintains regular contact with narcotics couriers in Chicago, and manages a network of cocaine and heroin distributors in Michigan. Ripley was convicted in the Kent County, Michigan, Circuit Court in 1994 on a charge of possession with intent to deliver cocaine and served 2 years in prison.

b. Hass, a 21 year old male, is one of Ripley's narcotics distributors in Grand Rapids. On October 12, 2004, as discussed below, Hass has sold cocaine on several occasions to a confidential source, who was working under the supervision of the DEA. Hass is an eighteen-year old with no known prior criminal history.

c. Langdon is a 24 year old female and Ripley's girlfriend. Langdon regularly attends narcotics-related transactions and meetings with Ripley, and serves as a "lookout" for law enforcement activity for Ripley in those situations. Langdon has no known prior criminal history.

d. Succrattao is a 20 year old male and one of Hass' cocaine customers, as observed by physical surveillance conducted by the GRPD and information from a confidential source. Succrattao has four prior felony convictions for possession of narcotics, most recently in 1999.

e. Gemink is a 26 year old male and one of Ripley's narcotics distributors. In July 2003, Gemink was interviewed by the GRPD in conjunction with a traffic stop of Gemink's vehicle for failure to stop at a traffic signal. Pursuant to a consent search GRPD officers found sixteen (16) ounces of cocaine in Gemink's vehicle. A felony possession of narcotics charge was filed against Gemink as a result of this incident, but was dismissed by the Kent County Prosecutor's Office before trial.

f. Paul, a 28 year old male, is one of Ripley's narcotics couriers. According to multiple confidential sources, Paul travels regularly between Grand Rapids and Chicago to transport narcotics and narcotics proceeds. Paul lives in the same apartment complex as Ripley, and was incarcerated with Ripley

from 1995 to 1996. Paul was convicted of a one count of felony possession of a firearm in 1995.

g. "Mr. C." is one of Ripley's Chicago-based narcotics trafficking associates. Based on consensually-recorded calls with a confidential source in which Ripley mentioned the movement of narcotics shipments from Chicago to Grand Rapids, I believe "Mr. C" is responsible for coordinating the shipment of narcotics and narcotics proceeds to and from Grand Rapids for the Ramirez Organization. No further identifying information is available for "Mr. C."

h. Raul LNU is a narcotics courier responsible for transporting narcotics from Texas to Chicago and Grand Rapids. No further identifying information is available for Raul LNU.

i. Regatto LNU is a narcotics courier responsible for transporting narcotics from Texas to Chicago and Grand Rapids. No further identifying information is available for Regatto LNU.

10. Ramirez is believed to be a mid-level cocaine and heroin supplier based in Mexico. A confidential source identified Ramirez as Raul LNU's and Regatto LNU's supervisor who directs the shipment of multi-kilogram quantities of cocaine and heroin from Mexico into Texas and ultimately to Chicago and Grand Rapids. I believe Ramirez attempts to insulate himself from detection from law enforcement by avoiding any direct narcotics-related discussions with any of the Chicago- and Grand Rapids-based **Target Violators**. Based on an analysis of telephone records and court-authorized wire interceptions, discussed below, I believe that Ramirez only speaks telephonically with Raul LNU, one of his narcotics couriers, regarding narcotics shipments sent to Chicago and Grand Rapids. Because Ramirez is not expected to be intercepted over **Target Phones 1 and 2** or over any **various and changing cellular telephones** used by Ripley, he has been named as a target violator, but as a target interceptee, in this affidavit.

III. FACTS ESTABLISHING PROBABLE CAUSE

A. SUMMARY OF PROBABLE CAUSE

11. The primary target of this investigation is the narcotics trafficking and money laundering organization led by Ramirez, including the Ramirez Organization's Chicago- and Grand Rapids-based Cells. The Ramirez Organization is involved in the smuggling of cocaine and heroin from Mexico into the United States. The Ramirez Organization, through lieutenants based in the United States, arranges for the transportation of shipments of cocaine and heroin to Chicago and Grand Rapids for further distribution. The Ramirez Organization also coordinates the laundering of narcotics proceeds and the return of these proceeds

from the United States to Mexico via the Chicago Cell and the Grand Rapids Cell.

12. The investigation has included the interception of wire communications over two cellular telephones ("Raul phones 1 and 2") used by Raul LNU pursuant to Title III orders issued by the United States District Court for the Southern District of Texas. The investigation has also included the use of three confidential sources ("CS-1" through "CS-3"). The information provided by CS-1 through CS-3 is believed to be reliable and has been corroborated through other investigative means, including consensually-recorded and/or consensually-monitored conversations, physical surveillance, and other investigative techniques.[22]

13. The investigation, including court-authorized wire interceptions over Raul phones 1 and 2 and information provided by CS-1 through CS-3, has revealed that Ripley is the leader of the Grand Rapids Cell, which distributes multi-kilogram quantities of cocaine and heroin to customers in and around the Grand Rapids, Michigan, area, and oversees the collection of narcotics proceeds from these customers; that "Mr. C." is a member of the Chicago Cell and directs the movement of narcotics and narcotics proceeds to and from Grand Rapids; that Ramirez directs the shipment of cocaine and heroin into the United States and the receipt of narcotics proceeds from the United States to Mexico; and that he uses Raul LNU and Regatto LNU as narcotics couriers to facilitate these activities.

14. The investigation has also revealed that since September 1, 2004, Ripley has used at least six different cellular telephones (collectively referred to as "Prior Phones 1 through 6"), not including **Target Phones 1 and 2.** Ripley has been intercepted engaging in narcotics-related conversations while using Prior Phones 3, 4, and 5. Additionally, CS-3 engaged in consensually-recorded, narcotics-related conversations with Ripley over Prior phones 1, 2, and 6. On January 3, 2005, DEA Grand Rapids obtained authorization to intercept wire

---

[22] All confidential sources included in the Title III affidavit must be qualified. Current Department policy requires that all informants used in the affidavit to establish probable cause be qualified according to the "Aguilar-Spinelli" standards (See, Aguilar v. Texas, 378 U.S. 108 (1964) and Spinelli v. United States, 393 U.S. 410 (1969)), rather than those set forth in the more recent Supreme Court decision of Illinois v. Gates, 463 U.S. 1237 (1983). Such qualification should include the statement that the confidential source(s) information is believed to be reliable and a statement regarding the amount of the corroboration of the confidential source(s) information. Additionally, any facts bearing on the credibility of the confidential source (e.g., to the extent promises of leniency, a criminal history involving crimes of dishonest, and any other factors considered pertinent by your circuit) should also be included in the affidavit so that the reviewing court can make an informed determination on the confidential source's credibility.

communications over Prior Phone 6. As discussed below, before those interceptions began, Ripley dropped Prior Phone 6. Based on intercepted calls over Raul phones 1 and 2, consensually-recorded calls made by CS-1 and CS-3, and the analysis of telephone records, the DEA believes that Ripley uses a cellular telephone for a short period of time and then discards that telephone in favor of a new cellular telephone, all with the effect of thwarting possible electronic surveillance being conducted by law enforcement. Additionally, based on wire interceptions over Raul phones 1 and 2 and consensually-recorded calls made by CS-1 and CS-3, the DEA believes that Ripley has recently begun compartmentalizing his use of cellular telephones, using separate telephones to communicate with his local distributors in Grand Rapids and other cellular telephones to communicate with his Chicago-based suppliers.

IV. USE OF PRIOR PHONES 1 THROUGH 6

A. PRIOR PHONE 1

15. The DEA identified Ripley as the user of Prior Phone 1 on September 3, 2004, when CS-3 revealed that Ripley used Prior Phone 1 to coordinate the shipment of narcotics from Chicago to Grand Rapids. An analysis of telephone records obtained from the service provider for Prior Phone 1 by subpoena revealed that Prior Phone 1 was activated on August 15, 2004. The first call made over Prior Phone 1 occurred on August 15, 2004. An analysis of telephone records revealed that Prior Phone 1 was not used again until September 1, 2004. Between September 1 and September 19, 2004, Prior Phone 1 was used to make and receive 547 calls. Based on my training and experience, I believe the initial call made over Prior Phone 1 on August 15, 2004, was completed to verify that Prior Phone 1 was properly activated, but that sustained use of Prior Phone 1 did not begin until on or about September 1, 2004.[23]

---

[23] In the case of a roving wire or electronic interception, 18 U.S.C. § 2518(b)(ii) requires a showing that the roving target uses various and changing facilities with the effect of thwarting electronic surveillance by law enforcement. This can be shown through informant information concerning the roving target's fear of wiretaps and his intention to use public telephones or cellular telephones to facilitate his criminal activities, combined with physical surveillance and/or telephone record analysis showing calls by the roving target to known or suspected criminal associates. In establishing this roving pattern, it is inadequate merely to allege that the roving target has been observed using several different pay telephones or cellular telephones and, therefore, must be effectively thwarting electronic surveillance. A sufficient factual basis must be established to permit the court to make the required finding that the roving target has effectively thwarted (optimally through a pattern covering weeks or months) the ability of law enforcement to conduct electronic surveillance by using various and changing facilities. It is not enough to show that the roving target has used a lot of different telephones. It must be established that the roving target has used a lot of different telephones to facilitate criminal activity. See, United States v. Gayton, 74 F.3d 545 (5th Cir.), cert. denied, 117 S. Ct. 77 (1996); United States v.

16. On September 6, 2004, under the supervision of a DEA agent, CS-3 called Prior Phone 1 and spoke with Ripley. During this consensually-recorded conversation[24], CS-3 asked about the timing of "the tractor" (referring to a semi-tractor trailer containing a shipment of narcotics)[25]. Ripley said that he had not spoken to "his boy (Mr. C.) in Chicago," but that he (Ripley) expected "it (the narcotics) to be here by the end of the week." CS-3 asked if "it (the narcotics shipment) was white (cocaine) or dark (heroin)." Ripley responded, "A bit of both (cocaine and heroin)." Later in the conversation, Ripley said that he would call CS-3 back when "it" (the narcotics shipment) arrived.

17. On September 15, 2004, Ripley, using Prior Phone 1 (as revealed by the caller identification feature on CS-3's cellular telephone and an analysis of toll records), called CS-3. During this consensually-recorded conversation, Ripley said, "It (the narcotics shipment) is here tomorrow....Not as much as I thought (referring to the quantity of narcotics), but it'll be here." CS-3 asked if he should call Ripley the next day about the narcotics shipment." Ripley responded, "I'll call you. I got me a new phone (believed to be referring to Prior Phone 2, as discussed below)."

Petti, 973 F.2d 1441 (9th Cir. 1992), cert. denied, 507 U.S. 1035 (1993); United States v. Villegas, 1993 WL 535013 (S.D.N.Y. Dec. 22, 1993)(unreported). Although the statute does not distinguish between public, cellular, and landline telephones, it is the Department's policy that, except in rare instances involving rapidly changing use of telephones located in hotel rooms or restaurants, only cellular or public pay phones may be targeted in a roving wiretap.

As a practical matter in establishing the pattern necessary to obtain roving authorization to intercept wire communications over various and changing cellular telephones, the following factual information should be obtained from the service provider(s) of the prior cellular telephones used by the roving target, as well as his/her currently used cellular telephones: (1) date of activation; (2) date of first use of the facility; (3) date the facility was identified by law enforcement as being used by the roving target; and (4) date of last use of the facility (i.e, the date the roving target dropped the phone). Additionally, facts establishing use of the prior phones by the roving target to facilitate his/her criminal activities should also be included in the affidavit (e.g., prior wire interceptions over other tapped phones, consensually-recorded calls made by informants, etc.). Finally, for each prior phone used by the roving target, the affidavit should reference any attempts to obtain regular Title III orders for those phones, and any actual interceptions and the success, if any, at implementing those efforts.

[24] All calls made by confidential sources referenced in the affidavit should be corroborated by noting if the conversation was consensually-recorded or consensually-monitored, and how the call was verified (e.g., toll records, pen register/trap and trace, agent dialing the target phone number, etc.)

[25] Coded conversations that the affiant believes are criminal in nature must be characterized in the affidavit with the law enforcement agent's belief (based on training and experience and the information obtained through the course of the investigation) regarding what the conversations actually mean.

18. A review of telephone records revealed that Prior Phone 1 was last used on September 19, 2004. Based on the calling records for Prior Phone 1, I believe that Ripley used Prior Phone 1 for a total of 19 days, and that he discarded Prior Phone 1 and replaced that facility with Prior Phone 2.[26]

B. PRIOR PHONE 2

19. The DEA identified Ripley as the user of Prior Phone 2 on September 18, 2004, when Ripley used Prior Phone 2 (as verified by toll records) to call CS-3. An analysis of telephone records obtained from the service provider for Prior Phone 2 by subpoena revealed that Prior Phone 2 was activated on September 13, 2004. The first call made over Prior Phone 2 occurred on September 14, 2004. Between September 14 and September 30, 2004 (the date of the last use), Prior Phone 2 was used to make and receive 346 calls.

20. On September 18, 2004, Ripley, using Prior Phone 2 (as verified by toll records) called CS-3. This call was not consensually-recorded. According to CS-3, Ripley said that "G" (Gemink) and Paul were collecting the "papers" (narcotics proceeds) to return to Chicago, and that the "tractor" (the tractor containing the cocaine and heroin shipment) was unloaded. Ripley said that "G" (Gemink) had noticed several suspicious vehicles near his house (believed to be a stash house where the Grand Rapids Cell stores narcotics) and that he (Gemink) thought the "heat (law enforcement) was about." Ripley told CS-3 to obtain a new telephone, and to stop calling him at his "old number" (referring to Prior phone 1).

21. A review of telephone records revealed that Prior Phone 2 was last used on September 30, 2004. An analysis of telephone records also revealed that the use of Prior Phone 2 was greatly curtailed beginning on September 26, 2004. Based on the calling records for Prior Phone 2, I believe that Ripley used Prior Phone 2 for a total of 17 days, and that he discarded Prior Phone 2 and replaced that facility with Prior Phone 3.

C. PRIOR PHONE 3

22. The DEA identified Ripley as the user of Prior Phone 3 on September 27, 2004, based on Title III interceptions over Raul phone 1. On September 10, 2004, DEA-Houston obtain court-authorization to intercept wire communications over Raul Phone 1. An analysis of telephone records obtained from the service provider for Prior Phone 3 by subpoena revealed that Prior Phone

---

[26] A more detailed telephone analysis is required when the roving target's use of that particular telephone cannot be established any other way (e.g., through confidential source information, ongoing Title III surveillance, etc.). The facts must show that the roving target has used the telephone in furtherance of the criminal conduct under investigation.

3 was activated on September 13, 2004, the same date on which Prior Phone 2 was activated. The first call made over Prior Phone 3 occurred on September 15, 2004. Between September 15 and September 28, 2004 (the date of the last use), Prior Phone 3 was used to make and receive 104 calls. Based on the fact that the service provider and activation dates for Prior Phones 2 and 3 are the same, I believe Ripley obtained Prior Phones 2 and 3 at the same time, but that Ripley did not begin using Prior Phone 3 until September 15, 2004.

23. On September 27, 2004, Raul LNU, using Raul Phone 1, called Prior Phone 3 and spoke with Ripley. Raul said that he was on "96" (referring to Interstate 96, the primary highway connecting Chicago and Grand Rapids), and that he expected to be at "the Grand" (Grand Rapids) within the hour. Ripley asked if Raul "had any troubles" (believed to be referring to law enforcement). Raul responded, "No troubles, man...the stuff (narcotics) is pura (high-quality). You are going to love it." Later in the conversation, Raul asked if Ripley had "spoken with Mr. C?" Ripley responded negatively. Raul said that "Mr. C. wants the papers (narcotics proceeds)...no more waiting, things need to go back (narcotics proceeds needed to be sent to Ramirez in Mexico)." Ripley said that he was "working on it (collecting the narcotics proceeds)," but that "they (the Chicago Cell and Ramirez) need to be patient."

24. As a result of court-authorized interceptions over Raul Phone 1, DEA Grand Rapids was able to conduct physical surveillance on September 27, 2004, of Raul LNU delivering approximately 30 kilograms of cocaine to Paul McManus (McManus) in Grand Rapids. On September 27, 2004, I observed a vehicle driven by Raul enter McManus' garage at 220 Spring Street, Grand Rapids, Michigan. Approximately ten minutes later, Raul's vehicle left the garage. On the night of September 27, 2004, based on wire interceptions over Raul Phone 1 and this physical surveillance, the GRPD and DEA executed a search warrant at McManus's residence and seized 30 kilograms of cocaine. McManus was arrested, remains in custody, and has not cooperated with law enforcement. Because he remains incarcerated, McManus has not been named as a Target Violator in this affidavit.

25. On September 28, 2004, Ripley, using Prior Phone 3, called Raul Phone 1 and spoke with Raul. Ripley said, "Yo, have you heard? They closed the door (referring to the seizure of the 30 kilograms of cocaine by law enforcement)." Raul responded, "What?" Ripley said, "Yeah, they closed the door at Paul's....slammed it (referring to the seizure of cocaine and McManus's arrest)." Raul said, "Shit, man....I've got to call C (referring to Mr. C., a high-ranking member of the Chicago Cell)." Later on the same date, Raul, using Raul Phone 1, spoke with "Mr. C," who was using a telephone located in Chicago (as revealed by cell-site records obtained from the service provider

for Mr. C.'s phone). Raul and Mr. C. discussed "the trouble in G.R." (referring to the seizure of the 30 kilograms of cocaine in Grand Rapids). Raul said that he would obtain a "new batch (of cellular telephones)...these are bad (referring to Raul Phone 1 and the cellular telephone used by Mr. C.)." Mr. C. responded affirmatively. Raul stopped using Raul Phone 1 on September 28, 2004. On October 10, 2004, DEA Houston obtained court-authorization to wiretap Raul Phone 2, Raul's replacement cellular telephone. Those interceptions continued until December 9, 2004, pursuant to a continuation order issued in the Southern District of Texas on November 10, 2004.

26. A review of telephone records revealed that Prior Phone 3 was last used on September 28, 2004. Based on the calling records for Prior Phone 3, I believe that Ripley used Prior Phone 3 for a total of 14 days, and that he discarded Prior Phone 3 and replaced that facility with Prior Phone 4.

D. PRIOR PHONE 4

27. The DEA identified Ripley as the user of Prior Phone 4 on October 15, 2004, based on Title III interceptions over Raul phone 2. An analysis of telephone records obtained from the service provider for Prior Phone 4 by subpoena revealed that Prior Phone 4 was activated on September 28, 2004, the day after the seizure of 30 kilograms of cocaine by law enforcement described above. The first call made over Prior Phone 4 occurred on September 28, 2004. Between September 28 and October 18, 2004 (the date of the last use of Prior Phone 4), Prior Phone 4 was used to make and receive 211 calls. Based on the activation date of Prior Phone 4 in close proximity to the cocaine seizure described above, I believe Ripley stopped using Prior phone 3 after the September 27, 2004, cocaine seizure and obtained Prior Phone 4 as his replacement cellular telephone.

28. On October 15, 2004, Ripley, using Prior Phone 4, called Raul Phone 2 and spoke with Raul. Raul said that "Regatto is driving this time (transporting a shipment of narcotics)," and that "he (Regatto) will arrive at the Tower (believed to be referring to Chicago, the location of the Sears Tower) on Sunday (October 16, 2004)." Ripley asked if Regatto would also be coming to Grand Rapids. Raul responded, "God willing, yes." Later in the conversation, Raul provided Ripley with a telephone number for a cellular telephone ("the Regatto phone") used by Regatto. An analysis of telephone records revealed that, approximately 15 minutes after the intercepted conversation between Raul and Ripley referenced above, Prior Phone 4 was used to call the Regatto phone. Based on the timing of this call, in conjunction with Raul's admission that Regatto was traveling to Chicago and Grand Rapids, I believe that Ripley called Regatto to discuss the status of a narcotics shipment.

29. A review of telephone records revealed that Prior

Phone 4 was last used on October 18, 2004. Based on the calling records for Prior Phone 4, I believe that Ripley used Prior Phone 4 for a total of 21 days, and that he discarded Prior Phone 4 and replaced that facility with Prior Phone 5.

E. PRIOR PHONE 5

30. The DEA identified Ripley as the user of Prior Phone 5 on November 1, 2004, based on court-authorized wire interceptions over Raul Phone 2. An analysis of telephone records obtained from the service provider for Prior Phone 5 by subpoena revealed that Prior Phone 5 was activated on October 21, 2004. The first call made over Prior Phone 5 occurred on October 22, 2004. Between October 22 and November 8, 2004 (the date of the last call over Prior Phone 5), Prior Phone 5 was used to make and receive 178 calls.

31. On November 1, 2004, Raul LNU, using Raul Phone 2, called Prior Phone 5 and spoke with Ripley. Raul asked how "the work is going (inquiring about the status of Ripley's narcotics trafficking activities)?" Ripley said that "things are slow...but I have all of those things (narcotics proceeds)." Raul said, "Good, you can give them to him (a narcotics courier, believed to be Regatto LNU) when he comes there." Ripley responded affirmatively, and asked "how many (units of narcotics) will be here?" Raul said, "At least 20 doves (20 kilograms of cocaine) and 10 of the dark (10 kilograms of heroin)." Raul asked "how many (narcotics proceeds) are coming back?" Ripley responded, "Two hundred" ($200,000 in narcotics proceeds).

32. On November 6, 2004, Raul, using Raul Phone 2, called Prior Phone 5 and spoke with Ripley. Raul said that "Regatto picked up a new number (a new cellular telephone). He will call you when he arrives." Ripley responded affirmatively. A review of telephone records for Prior Phone 5 on November 6 and 7, 2004 revealed that Prior Phone 5 was used to make and receive 15 calls to and from a cellular telephone (Regatto Phone 2) assigned area code (713), an area code normally associated with the Houston, Texas, area. A review of cell cite information obtained via a 2703(d) order for Regatto Phone 2 revealed that Regatto Phone 2 was being used between Chicago and Grand Rapids between November 6 and 7, 2004. Based on this information, I believe that Ripley used Prior Phone 5 to make and receive calls to/from Regatto Phone 2, and discussed a pending narcotics shipment being transported by Regatto.

33. On November 7, 2004, Raul LNU, using Raul Phone 2, called Prior Phone 5 and spoke with Ripley. Raul asked if Ripley had "seen Regatto." Ripley responded affirmatively, and said that "things (the narcotics delivered by Regatto) looked good."

34. A review of telephone records revealed that Prior

Phone 5 was last used on November 8, 2004, the day after Regatto delivered the narcotics shipment described above. Based on the calling records for Prior Phone 5, I believe that Ripley used Prior Phone 5 for a total of 17 days, and that he discarded Prior Phone 5 and replaced that facility with Prior Phone 6.

F. PRIOR PHONE 6

35. The DEA identified Ripley as the user of Prior Phone 6 on November 15, 2004, based on an analysis of pen register and trap and trace records for Regatto Phone 2 and confidential source information. A review of telephone records for Reggato phone on November 15, 2004, revealed 3 incoming calls from the telephone number assigned to Prior Phone 6, a telephone number that had not previously appeared on the trap and trace device monitoring Raul Phone 2. Based on this information, CS-3, under the supervision of the DEA, engaged in a consensually-recorded meeting with Ripley at a bar in Grand Rapids. CS-3 asked about purchasing "a quarter" (one-quarter kilogram of cocaine) from Ripley. Ripley said that he could "get that" (the cocaine) for CS-3, but that it would cost more because Ripley had to "break it (a full kilogram of cocaine) up." CS-3 asked how he should contact Ripley. Ripley provided the telephone number assigned to Prior Phone 6 to CS-3.

36. An analysis of telephone records obtained via subpoena revealed that Prior Phone 6 was activated and first used on November 9, 2004, the day after the last use of Prior Phone 5. Between November 9 and December 2, 2004 (the date of the last use of Prior Phone 6), Prior Phone 6 was used to make and receive 411 calls. Based on the close proximity of the activation date of Prior Phone 6 to the delivery of narcotics by Regatto on November 8, 2004, I believe that Ripley stopped using Prior Phone 5 following his receipt of cocaine from Regatto, and that he obtained Prior Phone 6 as his replacement cellular telephone.

37. On December 2, 2004, CS-3, under the supervision of a DEA Special Agent, called Prior Phone 6 and spoke with Ripley. CS-3 asked if he could "get that" (one-quarter kilogram of cocaine). Ripley responded affirmatively, and said that he would meet CS-3 at "the Beltline" (a bar in Grand Rapids). CS-3 asked what "the damage" (the price for the cocaine) would be. Ripley responded, "Eight" ($8,000). CS-3 and Ripley agreed to meet later that night.

38. Later on December 2, 2004, CS-3, under the supervision of the DEA, went to the prearranged meeting location to purchase cocaine from Ripley. While CS-3 waited in the parking lot at the bar, Ripley, using Prior Phone 6 (as verified by the caller identification feature on CS-3's cellular telephone and telephone records) called CS-3. During this consensually-recorded conversation, Ripley asked, "Did you see that van?" CS-3 responded negatively. Ripley said, "Forget it...it's no good."

Ripley was observed by physical surveillance units leaving the scene. Based on my training and experience, I believe that Ripley noticed a blue van near CS-3's location which contained DEA agents conducting physical surveillance of the area. The DEA attempted to follow Ripley from the scene, but was unable to so due to counter-surveillance measures implemented by Ripley, including several U-turns and driving down a one-way street. Since this incident, Ripley has rebuffed several attempts by CS-3 to meet with him.

39. On December 4, 2004, DEA Grand Rapids obtained court authorization to wiretap Prior Phone 6 from this court. Before that order could be implemented, the DEA learned (based on an analysis of telephone records) that Ripley had dropped Prior Phone 6. A review of telephone records revealed that Prior Phone 6 was last used on December 2, 2004. In fact, calling records for Prior Phone 6 revealed that the last call made from Prior Phone 6 was the call made from Ripley to CS-3 immediately prior to their scheduled narcotics transaction described above. Based on the calling records for Prior Phone 6, I believe that Ripley used Prior Phone 6 for a total of 24 days, and that he discarded Prior Phone 6 and replaced that facility with **Target Phones 1 and 2**. I also believe that Ripley discarded Prior Phone 6 and obtained **Target Phones 1 and 2** as a result of his belief that law enforcement was conducting physical surveillance of his illegal activities.

40. The following table summarizes Ripley's use of Prior Phones 1 through 6:

Phone	Activation	1st Use	Last Use	Total Days Used
PP1	08/15/04	09/01/04	09/19/04	19
PP2	09/13/04	09/14/04	09/30/04	17
PP3	09/13/04	09/15/04	09/28/04	14
PP4	09/28/04	09/28/05	10/18/04	21
PP5	10/21/04	10/22/04	11/8/04	17
PP6	11/9/04	11/9/04	12/2/04	24

V. USE OF TARGET PHONES 1 AND 2

A. TARGET PHONE 1

41. The DEA identified Ripley as the user of Target Phone 1 on December 7, 2004, based on court-authorized wire interceptions over Raul Phone 2. An analysis of telephone records obtained from the service provider for Target Phone 1 by subpoena revealed that Target Phone 1 was activated on December 3, 2004, the day after the scheduled meeting between CS-3 and Ripley described above. The first call made over Target Phone 1

occurred on December 4, 2004. Since December 4, 2004, Target Phone 1 has been used to make and receive 203 calls.

42. On December 7, 2004, Ripley, using Target Phone 1, called Raul Phone 2 and spoke with Raul. Ripley said that things were "heating up" (referring to an increased focus from law enforcement), but that he (Ripley) wanted to "keep things going (obtain more narcotics)." Raul responded affirmatively, and said that Ripley needed "to talk with C (Mr. C, a member of the Chicago Cell)." Raul said that he would have Mr. C. call Ripley.

43. On December 10, 2004, Raul, using Raul Phone 2, called Target Phone 1 and spoke with Ripley. Raul said that "the truck (a shipment of narcotics) was leaving Houston." Ripley asked when "it" (the narcotics shipment) would "reach the lake (believed to be referring to Lake Michigan and Chicago)." Raul said that the narcotics shipment would "take a few days." Ripley responded affirmatively.

B. <u>TARGET PHONE 2</u>

44. The DEA identified Ripley as the user of Target Phone 2 on December 9, 2004, based on information provided by CS-1 and an analysis of telephone records. On December 9, 2004, CS-1 met with Hass, one of Ripley's narcotics distributors, to purchase one-quarter kilogram of cocaine. During this consensually-recorded meeting, CS-1 asked about purchasing one-half kilogram of cocaine. Hass said that he did not have any more cocaine, but that he would call his "man" (supplier). In the presence of CS-1, Hass used his cellular telephone ("the Hass Phone") to call Target Phone 2 (as verified by telephone records). CS-1 overheard Hass' portion of the conversation. Hass said that he needed "another fourth (one-quarter kilogram of cocaine)." After Hass ended his telephone conversation, he told CS-1 that "Jack (Ripley) said he'd have it (the cocaine) tonight."

45. On December 11, 2004, CS-1, under the supervision of the DEA, called the Hass Phone and spoke with Hass. During this consensually-recorded conversation, CS-1 asked about purchasing an additional "one-quarter" (one-quarter kilogram of cocaine). Hass said that he would call CS-1 back in a few minutes. An analysis of telephone records revealed that, immediately after CS-1's telephone conversation with Hass, the Hass Phone was used to call Target Phone 2. Telephone records reveal that his call lasted approximately two (2) minutes. Minutes after the call to Target Phone 2, Hass, using the Hass Phone (as verified by the caller identification feature on CS-1's telephone), called CS-1 back. Hass said that "it (obtaining the one-quarter kilogram of cocaine) is no problem." CS-1 agreed to meet Hass later that night to consummate the cocaine transaction.

46. An analysis of telephone records obtained via

the service provider for Target Phone 2 revealed that Target Phone 2 was activated and first used on December 5, 2004. Since December 5, 2004, Target Phone 2 has been used to make and receive 307 calls, all to/from telephones assigned Michigan area codes. Based on this information, I believe that Ripley has compartmentalized his use of **Target Phones 1 and 2**, using Target Phone 1 to communicate with his Chicago and Texas co-conspirators, and Target Phone 2 to facilitate the distribution of narcotics in Michigan.

VI. PEN REGISTER AND TOLL RECORDS FOR TARGET PHONES 1 AND 2

47. In connection with this investigation, I have obtained and reviewed toll records for **Target Phones 1 and 2** for the period from on or about December 5 through on or about December 14, 2004. Additionally, on December 10, 2004, this court authorized the use of a pen register/trap and trace device to monitor incoming and outgoing telephone numbers of calls made over **Target Phones 1 and 2.** These records demonstrate that **Target Phones 1 and 2** are being used to contact other members of the Rodriguez Organization, including members of the Chicago and Grand Rapids Cells.

48. For example, toll records and pen register/trap and trace data show that **Target Phone 1** has been used to make and/or receive the following pertinent calls:

a. 22 calls to and from a cellular telephone used by "Mr. C," a high-ranking member of the Chicago Cell, as identified in court-authorized wire interceptions over Raul Phone 2, with the most recent call on December 14, 2004[27];

b. 11 calls to and from an un-tapped[28] landline telephone used by Raul LNU, with the most recent call on December 9, 2004;

---

[27] All identified individuals with telephones being contacted by the target phone(s) that are referenced in the toll/pen analysis section of the affidavit should be named as both target violators and target interceptees in the affidavit. By including this information, the affiant is implying to the court that these individuals are involved in the criminal offenses under investigation and are making and/or receiving calls to and from the target phone(s).

[28] Contact made by the target phone(s) to and from wiretapped telephones (or phones used by confidential sources) may be included in the toll/pen analysis. However, contacts made from the target phone(s) to and from these telephones, standing alone, do not satisfy the Department's policy pertaining to telephone records analysis (commonly referred to as the "21 day rule"). While such contacts are relevant to the finding of probable cause that the target phone(s) is being used to facilitate the predicate offenses, the necessity element of the statute must also be satisfied. Contacts to and/or from "dirty" telephones that law enforcement would be missing without a wiretap on the target phone(s) must be shown to satisfy the necessity requirement of the statute, except in rare instances when the particular investigative facts warrant otherwise.

c. nine (9) calls to and from a telephone used by RegattoLNU, one of the Ramirez Organization's narcotics couriers, as identified in court-authorized wire interceptions over Raul Phone 2, with the most recent call on December 10, 2004; and

d. 31 calls to and from three prepaid cellular telephones used primarily in the Chicago, Illinois, area (as revealed by cell site information subpoenaed from the service providers), with the most recent call to one of the prepaid phones on December 14, 2004. Because no subscriber information is available for these telephones, the DEA is unaware of the actual users of these telephones. Additionally, I am aware that narcotics traffickers often obtain prepaid cellular telephones or use fictitious subscriber information in an attempt to hide their identities from law enforcement. Given the detailed information in this investigation that Ripley receives large quantities of narcotics from the Chicago, Illinois, area, and that Ripley sends large amounts of narcotics proceeds to the Chicago Cell, I believe that some of the calls made to these three (3) Chicago prepaid cellular telephones are related to Ripley's narcotics trafficking activities.

49. Toll records and pen register/trap and trace data show that Target Phone 2 has been used to make and/or receive the following pertinent calls:

a. 23 calls to and from the Hass Phone, one of Ripley's narcotics distributors (as identified above), with the most recent call on December 14, 2004;

b. 38 calls to and from a cellular telephone used by Langdon, with the most recent call on December 14, 2004. According to CS-3, Langdon is Ripley's girlfriend and has attended narcotics-related meetings with Ripley and served as a lookout for law enforcement activity on those occasions.

c. three (3) calls to and from a landline telephone used by Succrattao, with the most recent call on December 6, 2004. According to CS-1, Succrattao is one of Hass' heroin customers, and oftentimes meets with Hass at his residence. Accordingly, I believe Ripley is using Target Phone 2 to engage in narcotics-related conversations with Hass and/or Succrattao over this telephone.

d. 12 calls to and from a cellular telephone used by Gemink, with the most recent call on December 12, 2004. As discussed above in ¶ 20, Ripley admitted to CS-3 that Gemink was one of his narcotics trafficking associates.

e. 15 calls to and from a cellular telephone used by Paul, an individual identified by CS-3 as one of Ripley's narcotics distributors in Grand Rapids, with the most recent call on December 14, 2004. According to CS-3, Paul lives in the same apartment complex and is one of Ripley's most trusted associates.

VII. ROVING PATTERN - USE OF VARIOUS AND CHANGING CELLULAR PHONES

50. As set forth above, since September 1, 2004, Ripley has used at least eight (8) different cellular telephones to facilitate his narcotics trafficking activities, including **Target Phones 1 and 2.** Ripley used Prior Phones 1 through 6 for, respectively, 19 days (Prior Phone 1); 17 days (Prior Phone 2); 14 days (Prior Phone 3); 21 days (Prior Phone 4); 17 days (Prior Phone 5); and 24 days (Prior Phone 6). On average, Ripley used the Prior Phones for approximately eighteen (18) days. Based on an analysis of telephone records, Ripley has used **Target Phones 1 and 2** for 16 and 15 days, respectively. Based on his established pattern of dropping cellular telephones, I believe Ripley will soon obtain new cellular telephones to replace **Target Phones 1 and 2.** Nonetheless, **Target Phones 1 and 2** remain the current telephones used by Ripley to facilitate his illegal activities.

51. Court-authorized wire interceptions, confidential source information, and the analysis of telephone records have confirmed that Ripley uses a particular cellular telephone extensively for a short period of time, and then drops that facility in favor of a new cellular telephone. As noted above, DEA Grand Rapids was able to obtain court-authorization to wiretap Prior Phone 6 on December 2, 2004, but Ripley dropped that facility before actual interceptions could begin. Ripley's short use of cellular telephones has effectively prevented the DEA from obtaining court-authorization to wiretap particular telephones used by Ripley, thus frustrating the DEA's attempts to intercept his calls. The time inherent in identifying Ripley's new cellular telephones, obtaining telephone records (from toll records and/or a pen register/trap and trace devices), analyzing telephone records, and obtaining court-authorization to wiretap Ripley's telephones, has had the effect of thwarting the DEA's ability to intercept the full scope of Ripley's wire communications regarding his narcotics trafficking activities.

52. The investigation to date has also revealed that Ripley changes cellular telephones on a regular basis in an attempt to avoid law enforcement scrutiny. As described above, Ripley has dropped cellular telephones in direct response to his perception that he was being targeted by law enforcement. Immediately prior to dropping Prior Phone 2, Ripley told CS-1 that he needed to obtain a new telephone because "the heat (law enforcement) was about." See, ¶ 20, above. Moreover, Ripley dropped Prior Phone 6 after spotting physical surveillance being conducted by the DEA. See, ¶ 38, above. Ripley has also dropped his cellular telephone in response to the seizure of narcotics by law enforcement. See, ¶¶ 23-25, above. Finally, Ripley has dropped cellular telephones regularly after receiving large quantities of narcotics from his associates in Chicago. See, ¶¶ 31-33, above. Based on these facts and my training and experience, I believe

that Ripley drops his cellular telephones on a regular basis in an attempt to thwart law enforcement's ability to intercept his communications, and that authorization to conduct roving interceptions of Ripley's wire communications is needed to develop the full scope of his narcotics trafficking activities.

VIII. NEED FOR WIRE INTERCEPTION

53. Based upon my training and experience, as well as the experience of other Special Agents of the DEA and other federal agents with whom I have consulted, in addition to the facts set forth in this affidavit, it is my belief that the interception of wire communications over **Target Phones 1 and 2** and the roving interception of wire communications over **various and changing cellular telephones** used by Ripley are the only available techniques that have a reasonable likelihood of developing the full scope of the Ramirez Organization's illegal activities and Ripley's role as the leader of the Grand Rapids Cell. Although law enforcement has been able to identify several of Ripley's co-conspirators and seized approximately 30 kilograms of cocaine, the identities of many co-conspirators remain unknown, including the true identities of the leaders of the Chicago Cell and other members of the Ramirez Organization. Moreover, wire interceptions will likely lead to more opportunities to conduct surveillance of Ripley and his associates, and assist in law enforcement's ability to interdict narcotics shipments and narcotics proceeds.

54. The following investigative techniques, which are usually applied in an investigation of this type, have been employed and have been unsuccessful, or reasonably appear unlikely to be successful if tried, or are too dangerous under the circumstances to be employed.

A. WIRETAPS OVER RAUL PHONES 1 AND 2 AND PRIOR PHONE 6

55. DEA Houston conducted court-authorized wire interceptions over Raul Phones 1 and 2 between September 10 and December 9, 2004. The interception of wire communications over Raul Phones 1 and 2 allowed the DEA to identify several of the Prior Phones used by Ripley. However, DEA Houston has advised me that Raul is no longer using Raul Phones 1 and 2, and the DEA has yet to ascertain the cellular telephones currently being used by Raul. Wiretapping **Target Phones 1 and 2 and various and changing cellular telephones used by Ripley** will likely assist in this endeavor. Moreover, interceptions over Raul Phones 1 and 2 did not reveal the full scope of Ripley's or the Chicago Cell's illegal activities. Those interceptions revealed that Ripley spoke with Raul sporadically, usually at or near the timing of shipments of narcotics to Grand Rapids or narcotics proceeds sent to Chicago. Telephone records reveal that Ripley uses the **Target Phones 1 and 2** to communicate regularly with co-conspirators

located in Grand Rapids and Chicago. Wiretapping **Target Phones 1 and 2 and various and changing cellular telephones used by Ripley** will allow the DEA to determine the full reach of the Ramirez Organization.

56. As discussed above, DEA Grand Rapids was able to obtain court-authorization to wiretap Prior Phone 6 on December 4, 2004. However, Ripley dropped that facility before interceptions could begin. Wiretapping **Target Phones 1 and 2 and various and changing cellular telephones used by Ripley** will allow the DEA to learn more about Ripley's illegal activities, as well as identify other telephones by Ripley to facilitate his illegal activities, and the identities and roles of his co-conspirators.

B. CONFIDENTIAL SOURCES

57. This investigation has employed several confidential sources, discussed above. While these sources continue to be useful in providing information on the general and historical operations of the Ramirez Organization and the Grand Rapids Cell in particular, the highly compartmentalized and international manner in which the Ramirez Organization does business has made it impossible for any of these sources to learn the identities of all the persons engaged in the varied criminal activities described above, particularly the intricate aspects of the narcotics trafficking and money laundering conducted by the Ramirez Organization across the United States. In addition, the information provided by the sources about certain criminal activities has not been received in advance of the actual criminal activity, making it impossible to identify all of the participants involved or to arrange in advance other investigative techniques, such as physical surveillance.

58. As discussed above, the investigation to date hasinvolved the use of CS-1, CS-2, and CS-3. However, they have only provided information regarding some of the **Target Violators**, and are not privy to all of their illegal activities. For example, CS-1 and CS-3 have only been able to provide information about the Grand Rapids Cell, and not about the larger Ramirez Organization, including the details of the operation of the Chicago Cell and the elements of the Ramirez Organization operating in Texas and Mexico. CS-2 has only been able to provide limited information on the Ramirez Organization's operations in Texas and, to a limited extent, Mexico. CS-2 has no knowledge of the Grand Rapids and Chicago Cells. Moreover, and perhaps most importantly, recent information has revealed that Ripley no longer will have any dealings with CS-3, the only confidential source that previously had direct dealings with Ripley. CS-1 has never had the ability to make direct contact with Ripley and has instead had dealings only with Ripley's lower level distributors. Accordingly, CS-1, CS-2, and CS-3 are only

in a position to provide piecemeal information about the Ramirez Organization. In addition, narcotics organizations are generally highly-compartmentalized, and it is generally impossible for an informant to gain access to all aspects of an organization's illegal activities. In particular, narcotics organizations are highly protective of their sources of supply, and it does not appear likely that the confidential sources used to date could facilitate the introduction of an undercover agent to Mexican sources of supply at this point. Confidential informants alone would likely be inadequate to develop evidence about the **Target Violators'** suppliers and customers. In addition, based on my experience as a narcotics investigator, I believe that drug traffickers are unlikely to discuss the full extent of their organization's activities or membership when dealing with "outsiders." With the limited information provided, to date, by the informants, and without the evidence obtained from court-authorized interceptions, the objectives of this investigation cannot be met.

C. PHYSICAL SURVEILLANCE

59. As described above, physical surveillance of certain of the **Target Violators** has been performed. However, based on my experience and training, and my participation in this investigation, narcotics traffickers who are at the level of the Ripley and his associates are extremely surveillance-conscious. Indeed, as discussed above, interceptions over Raul Phones 1 and 2 and information provided by CS-1 and CS-3 have revealed that the Ripley and the other **Target Violators** are actively engaged in sophisticated counter-surveillance techniques. For example, during the his scheduled December 2, 2004, meeting with CS-3, Ripley exhibited numerous counter-surveillance driving techniques. Further, information from CS-3 has revealed that Ripley uses "lookouts" as a method of detecting physical surveillance being conducted by law enforcement. Ripley currently lives in a gated apartment complex that is located on a cul-de-sac road that makes stationary physical surveillance extremely difficult. Wire interceptions and source information have also revealed that the Ramirez Organization is highly suspicious of law enforcement activity. Accordingly, increased surveillance could alert the **Target Violators** to the existence of the investigation, and cause them to relocate or temporarily cease their illegal activities, thereby hindering the investigation. It is expected that the information that can be obtained from the interception of wire communications over the **Target Phones 1 and 2** and roving interceptions over **various and changing cellular telephones** used by Ripley will help law enforcement agents locate the identified **Target Violators** and identify additional **Target Violators**, and thereby enhance the prospects for fruitful physical surveillance. In addition, with

the knowledge provided beforehand by wire surveillance that a meeting is to take place at a given location, it may be possible to establish physical surveillance at that location in advance, thus minimizing the risks of discovery inherent in following subjects or remaining at target locations for extended periods of time.

60. In addition, at least some of the **Target Violators** and their associates are located in or operate extensively in Mexico, where U.S. agents cannot perform surveillance without the assistance of Mexican authorities via Mutual Legal Assistance Treaty request. Wire interception is the only feasible means of learning about the illegal activities of these Mexico-based targets, and about the Mexican operations of the **Target Violators**. Accordingly, intercepting communications to and from the **Target Phones 1 and 2** and roving interception of wire communications over **various and changing cellular telephones used by Ripley** will provide direct evidence of communications between the **Target Violators** and other conspirators and assist in identifying **Target Violators**, including suppliers of narcotics to the **Target Violators**; locations from which they conduct their activities and store cash and narcotics; and additional narcotics customers of the **Target Violators** -- information that surveillance to date has not yet fully revealed.

D. PEN REGISTER/TRAP AND TRACE AND TOLL RECORDS

61. Telephone toll records and pen register/trap and tracedata have been used and are continuing to be used in this investigation, as described above, and, in fact, will be important to help identify new telephones being used by Ripley or to corroborate such use. These records and data have verified frequent telephone communication between **Target Phones 1 and 2** and other telephones used by members of the Ramirez Organization. However toll records and pen registers and trap and trace devices provide only limited information. Pen registers/trap and traces and toll records do not necessarily assist with the identification of the parties to the conversation, do not provide the nature or substance of the conversation, and do not differentiate between non-criminal calls and calls for criminal purposes. Moreover, these records alone do not identify the source or sources of the controlled substances, nor do they alone establish proof of the conspiracy. Among other problems, a telephone number appearing in the records may not be listed or subscribed in the name(s) or address(es) of the person(s) using the telephone. Furthermore, the using of calling cards and telephone access numbers hides the ultimate numbers called thereby preventing the DEA from learning who the **Target Violators** are speaking with.

62. Wire interceptions over **Target Phones 1 and 2** and roving wire interceptions over **various and changing telephones used by Ripley** will provide direct evidence of the target offenses, and allow a greater opportunity to fully dismantle the Ramirez Organization.

E. FEDERAL GRAND JURY

_____63. Use of a federal grand jury does not appear to be a promising method of investigation. The issuance of grand jury subpoenas likely would not lead to the discovery of critical information and undoubtedly would alert the **Target Violators** to the existence of this investigation. Witnesses who could provide additional relevant evidence to a grand jury either have not been identified or would themselves be participants in the narcotics trafficking. Such individuals would face prosecution themselves; it is unlikely therefore that any of them would testify voluntarily and they would likely be uncooperative and invoke their Fifth Amendment privilege not to testify. Nor would it be desirable at this time to seek immunity for such individuals and to compel their testimony. Immunizing them could thwart the public policy that they be held accountable for their crimes. Moreover, the granting of such immunity might foreclose prosecution of the most culpable members of this conspiracy and could not ensure that such immunized witnesses would provide truthful testimony. It is also likely that such subjects would go into contempt rather than testify. The issuance of grand jury subpoenas to other individuals likely would not lead to the discovery of critical information and undoubtedly would alert the **Target Violators** to the pendency of an investigation. Moreover, not all of the **Target Violators** have been identified and, in the absence of further evidence identifying all of the co-conspirators and their respective involvement in drug trafficking, it is difficult to determine whom to subpoena to the Grand Jury.[29]

F. INTERVIEWS OF SUBJECTS OR WITNESSES

64. Based upon my experience, I believe that interviews of the **Target Violators** or their known associates would produce insufficient information as to the identities of all of the persons involved with the **Target Violators** in narcotics trafficking, the source of the drugs, the sources of financing, the location of records and drugs, and other pertinent information regarding the **Target Offenses**. I also believe that any responses to the interviews would contain a significant

---

[29] To the extent that additional facts exist regarding the grand jury (e.g., the use of grand jury subpoenas, etc.), an analysis should be included in the necessity portion of the affidavit. Also, if anyone has, in fact, been indicted, or if indictments will soon be sought, that information should be included.

number of untruths, diverting the investigation with false leads or otherwise frustrating the investigation. Additionally, questioning any of the co-conspirators would alert the other co-conspirators, and cause a change in their methods of operation before all of the co-conspirators are identified, thereby compromising the investigation and resulting in the possible destruction or concealment of documents and other evidence, and the possibility of harm to cooperating sources whose identities may become known or whose existence may otherwise be compromised.

65. As discussed above, on September 27, 2004, the GRPD arrested McManus after Raul LNU delivered approximately 30 kilograms of cocaine to McManus' residence in Grand Rapids. The GRPD attempted to interview McManus regarding his involvement in the Ramirez Organization on September 27, 2004, but he immediately invoke his Fifth Amendment rights and informed GRPD officers that he would not cooperate with them. Additionally, wire interceptions over Raul Phones 1 and 2 and information provided by CS-1, CS-2, and CS-3 have revealed several individuals who are acquainted with the **Target Violators** in Texas, Chicago, and Grand Rapids. While it is theoretically possible to interview the **Target Violators'** friends and acquaintances, to do so would make the **Target Violators** aware of the existence of this investigation. Accordingly, I believe that interviews are not a viable investigative technique at this stage of the investigation.

G. UNDERCOVER AGENTS

66. There is currently no expectation that an undercoverofficer will be able to determine the full scope of the **Target Violators'** operations, meet and identify all of the other **Target Violators** and their co-conspirators in Grand Rapids, Chicago, Texas, and Mexico, or identify all of the **Target Violators'** narcotics suppliers and their confederates. Based on my experience as a narcotics investigator, I believe that drug traffickers are unlikely to discuss the full extent of their organization's activities or membership when dealing with an "outsider" such as an undercover officer. In my experience, narcotics traffickers are usually highly reticent about discussing narcotics with unknown persons. In addition, the insertion of an undercover officer would involve unacceptable security risks. Further none of the confidential sources available to the DEA are in the position to introduce an undercover agent to Ripley or the other high-ranking members of the Ramirez Organization.

67. For example, on December 3, 2004, CS-1 met with Hass, one of Ripley's narcotics distributors in Grand Rapids, and discussed purchasing cocaine. During this consensually-recorded meeting, CS-1 asked about meeting Hass' "boy" (narcotics supplier). Hass said that "he (Ripley, Hass' narcotics supplier)

deals with me, no one else." Based on this information, I believe that Ripley attempts to insulate himself from law enforcement activity by refusing to meet with people that he does not know for narcotics trafficking purposes. Further, given the fact that CS-3, the one source who had a personal relationship with Ripley, no longer has the ability to contact Ripley, it is impossible to introduce and undercover agent to Ripley to further the goals of the investigation.

H. SEARCH WARRANTS AND SEIZURES

68. Although law enforcement has seized approximately 30 kilograms of cocaine from the Grand Rapids Cell, further applications for search warrants are not appropriate at this stage of the investigation, as all of the locations where the **Target Violators** currently receive, hide, and distribute their narcotics and narcotics proceeds have not been identified. Moreover, investigative methods used to date do not by themselves seem likely to yield this information. Wire surveillance will assist law enforcement in identifying such locations, so that search warrants for such locations may be obtained at a later time in a coordinated effort aimed at disabling the Ramirez Organization's narcotics trafficking cells in Texas, Chicago, Grand Rapids, and in other possible locations across the United States.

69. As discussed above, on September 27, 2004, the GRPD seized approximately 30 kilograms of cocaine from McManus, a former member of the Grand Rapids Cell. Even with this seizure of narcotics, law enforcement was not able to identify all of the members of the nationwide Ramirez Organization, and has not been able to arrest or charge all **Target Violators** and **Target Interceptees** in this investigation. Moreover, law enforcement is still attempting to identify certain individuals that Ripley is in contact with through **Target Phones 1** and **2**, and over **various and changing cellular telephones being used by Ripley**. I believe that the execution of more search warrants at this time would likely compromise the investigation by alerting the **Target Violators** to the existence of the investigation, thereby allowing unidentified co-conspirators to further insulate themselves from detection, and to otherwise impede this investigation. While search warrants and interdiction of narcotics shipments and narcotics proceeds will likely occur in the future, such investigative techniques are best carried out in conjunction with wire interceptions. Wire interceptions will provided detailed information on the timing and location of narcotics shipments, and allow law enforcement to carry out systematic, nationwide interdiction of narcotics and narcotics proceeds.

I. ARRESTS

70. Attempting to arrest the **Target Violators** now would mean that several of the objectives of this investigation would be unfulfilled. Many of the **Target Violators** and their associates have yet to be identified or located, particularly the members of the Chicago Cell. If we arrested those **Target Violators** that have been identified, their unidentified co-conspirators would almost certainly temporarily cease their illegal activities or change instrumentalities and methods used to conduct their illegal activities. Moreover, although there is now probable cause to believe that the **Target Violators** are engaged in narcotics trafficking, the likelihood of convicting the **Target Violators** that have been identified of narcotics charges would be increased by evidence obtained from the requested surveillance.

71. As discussed above, the GRPD arrested one member of the Ramirez Organization, McManus, on September 27, 2004. The Grand Rapids Cell's response to that arrest is indicative of how the Ramirez Organization would likely respond to further arrests of the **Target Violators**. For example, Raul LNU and Ripley immediately obtained new cellular telephones after McManus' arrest and increased their efforts at avoiding law enforcement scrutiny. This response by the **Target Violators** underscores the need for authorization to intercept wire communications over **Target Phones 1 and 2**, as well as authorization to conduct roving wire interceptions over **various and changing cellular telephones** used by Ripley. Such interceptions will allow the DEA to fully identify and locate more members of the Ramirez Organization, and allow large scale arrests once this information has been developed.[30]

IX. PRIOR APPLICATIONS[31]

72. Reviews of the Electronic Surveillance Indices, located at the headquarters of the FBI, the Drug Enforcement Administration (DEA), and Immigration and Customs Enforcement (ICE), completed as of December 9, 2004, revealed that there have been no prior applications for authorization to intercept, or approvals of applications to intercept, wire, oral, or electronic communications involving any of the **Violators**, **Interceptees**, or **Target Phones 1 and 2** except as follows:

---

[30] If other investigative techniques have been pursued (e.g., pole cameras, trash searches, etc.) a specific discussion of these techniques in the necessity section of the affidavit must be included.

[31] All target violators, not just target interceptees, should be checked in the FBI, DEA, and ICE electronic surveillance records indices. Additionally, any targeted facility should also be checked. To the extent that any state or foreign wiretaps are known the investigative agents, those prior wiretaps should also be included in the prior application section of the affidavit.

a. On September 10, 2004, the United States District Court for the Southern District of Texas issued an order authorizing the interception of wire communications over Raul Phone 1. Those interceptions terminated on September 28, 2004, as discussed above. Raul LNU, Regatto LNU, "Mr. C.," and Ripley were named as target subjects in that applications, and were intercepted during that wiretap.

b. On October 10, 2004, the same court issued an order authorizing the interception of wire communications over Raul Phone 1. An order authorizing the continued interception of wire communications over Raul Phone 2 was issued by the same court on November 10, 2004. Those interceptions terminated on December 9, 2004. Raul LNU, Regatto LNU, "Mr. C.," and Ripley were named as target subjects in those applications, and were intercepted during those wiretaps.

c. On December 4, 2004, the United States District Court for the Western District of Michigan issued an order authorizing the original interception of wire communications over Prior Phone 6. All of the current **Target Violators** were named as **Target Violators** in that authorization. No interceptions occurred pursuant to this order, as Ripley dropped Prior Phone 6 before the interceptions could begin. The affidavit submitted in support of that application is incorporated by reference into the current affidavit.

X. MINIMIZATION

73. All monitoring of wire communications over **Target Phones 1 and 2** and **various and changing cellular telephones** used by Ripley will be minimized in accordance with Chapter 119 of Title 18, United States Code.[32]

74. The "investigative or law enforcement officers of the United States" and translators, if necessary, who are to carry

---

[32] The roving provisions of Title III have an "ascertainment" requirement. Namely, law enforcement must definitively ascertain and identify the "various and changing" cellular telephones used by the roving target before wire interceptions can begin over those facilities pursuant to the roving authorization. Identification of these telephones can take the form of confidential source information, wire interceptions over other tapped phones, physical surveillance, pretext calls, or other detailed information. Generally, telephone record analysis (i.e., a common call analysis), standing alone, is not sufficient to ascertain the roving target's use of a particular telephone.

Once a new telephone is ascertained and definitively placed in the hands of the roving target, wire interceptions over that facility can commence pursuant to the roving authorization by serving a copy of the redacted interception order on the service provider for the new cellular telephone. Additionally, a special report should be submitted to the authorizing court detailing the new cellular telephone used by the roving target, as well as the method(s) used to identify the roving target as the user of that facility.

out the requested interception of wire communications, will be instructed concerning the steps they should take to avoid infringing upon any attorney-client privilege or other recognized privileges. In addition, all communications intercepted will be conducted in such a way as to minimize the interception of communications not otherwise criminal in nature or subject to interception under Chapter 119, Title 18, United States Code. All monitoring will cease when it is determined that the monitored conversation is not criminal in nature. Interception will be suspended immediately when it is determined through voice identification, physical surveillance, or otherwise, that **Target Violators** or any of their confederates, when identified, are participants in the conversation, unless it is determined during the portion of the conversation already overheard that the conversation is criminal in nature. If an interception is minimized, monitoring agents shall spot check to insure that the conversation has not turned to criminal matters.

75. It is requested that the order provide that, if necessary, translators be authorized to assist in conducting this wire surveillance and to receive disclosure of intercepted communications. Certain subjects of this investigation are expected to communicate with each other in Spanish. It is therefore necessary to secure the services of translators in order to assist the agents in monitoring the wire surveillance and translating the intercepted communications. All such translators will be under contract to the law enforcement agencies involved in this case and will be directly supervised by the DEA. It is further requested, pursuant to Section 2518(5), Title 18, United States Code, that in the event the intercepted communications are in a code or foreign language, and an expert in that code or foreign language is not reasonably available during the interception period, that minimization may be accomplished as soon as practicable after such interception.

XI. AUTHORIZATION REQUEST

76. Based on the foregoing, it is my opinion that the interception of wire communications occurring over **Target Phones 1 and 2** and **various and changing cellular telephones** used by Jacob Ripley is essential to aid in the discovery of the full scope of the **Target Violators'** illegal activities.

77. IT IS HEREBY REQUESTED that an Order be issued authorizing special agents of the DEA, and other "investigative or law enforcement officers," as defined in Section 2510(7) of Title 18, United States Code, to intercept and record wire communications occurring over:

a. the prepaid cellular telephone bearing the number (616) 555-6068, subscribed to by Janis Jenkins, 1555 N. Shore Rd.,

Grand Haven, Michigan, and accessed through international mobile subscriber identification ("IMSI") number 316000115672568; and

b. the cellular telephone bearing the number (616) 555-6015, subscribed to by Steven Hill, 512 S. Division Street, Grand Rapids, Michigan, and assigned electronic serial number ("ESN") 345678000; and

c. various and changing cellular telephones used by Jacob Ripley, pursuant to Title 18, United States Code, Section 2518(11)(b).

78. The authorization requested is intended to apply not only to the target telephone numbers listed above, but to any other telephone numbers or telephones accessed through the above-referenced IMSI number, to any other IMSI numbers accessed through the target telephone number referenced above, to any other telephone numbers subsequently assigned to the instrument bearing the same electronic serial number as the other target cellular telephone listed above, and to any other cellular telephone used by Jacob Ripley within the authorization period. The requested authorization is also intended to apply to background conversations intercepted in the vicinity of the target telephones and to any other cellular telephone used by Jacob Ripley while the telephones are off the hook or otherwise in use.

79. IT IS HEREBY REQUESTED that such interceptions not automatically terminate when the type of communications described above have first been obtained, but be permitted to continue until all communications are intercepted that reveal the manner in which the **Target Violators** and others yet unknown participate in the above-described offenses, or for a period of 30 days, whichever is earlier, the 30 days commencing on the earlier of the day on which investigative or law enforcement officers first begin to conduct the interception or 10 days from the date of the Order.

80. Pursuant to the provisions of Title 18, United States Code, Sections 2518(4), it is requested that it be ordered that T-Mobile and Sprint, the service providers for **Target Phones 1 and 2**, and any other service providers for the **Target Phones 1 and 2** or any **various and changing cellular telephone used by Jacob Ripley**, furnish the technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with such services as those providers accord the persons whose communications are to be intercepted (including all dial digits for both incoming and outgoing calls), pen register information, and audio interception capability), and access to the **Target Phones 1 and 2** and **various and changing cellular telephones used by Jacob Ripley** voicemail boxes or voicemail features to intercept messages left on or retrieved from **Target Phones 1 and 2** voicemail boxes or voicemail systems on a realtime basis. The assistance of T-Mobile, Sprint, and any other service provider is required to

accomplish the objectives of the REQUESTED interceptions. Reasonable expenses incurred pursuant to this activity will be processed for payment by the DEA.

81. IT IS HEREBY REQUESTED that, because cellular phones are easily transported across district lines, it is requested that interceptions may occur not only within the jurisdiction of the court in which this application is being made, but outside that jurisdiction (but within the United States). Therefore, it is further requested that the interception not be terminated when any of the cellular phones is carried outside of the Western District of Michigan. In addition, because the use of a cellular telephone outside the usual service area of the respective service providers may result in the provision of service by other cellular service providers (known commonly as "roaming"), it is requested that the Order apply to any cellular service provider providing service to a telephone facility used by Ripley.

82. IT IS HEREBY FURTHER REQUESTED that this Affidavit, because it reveals an ongoing investigation, be sealed until further order of the Court. Sealing the Affidavit will help prevent premature disclosure of the investigation, guard against targets' becoming fugitives, and better ensure the safety of law enforcement agents and others.

_____

J. KENNETH SMITH

Special Agent

United States Drug Enforcement Administration

Sworn to before me this

_____ day of January, 2004

Application for Approval of Emergency Interception of Wire, Oral or Electronic Communications Under 18 U.S.C. 2518(7)

UNITED STATES DISTRICT COURT

_____DISTRICT OF_____

IN THE MATTER OF THE APPLICATION	)
OF THE UNITED STATES OF AMERICA FOR	)
AN ORDER APPROVING THE EMERGENCY	)
INTERCEPTION OF(WIRE)(ORAL)(ELECTRONIC)	)
COMMUNICATIONS	)
	)

APPLICATION FOR AN ORDER APPROVING THE EMERGENCY INTERCEPTION OF (WIRE)(ORAL)(ELECTRONIC) COMMUNICATIONS

_____, Assistant United States Attorney, _____ District of _____, being duly sworn, states:

1. I am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code, that is, an attorney authorized by law to prosecute or participate in the prosecution of offenses enumerated in Section 2516 of Title 18, United States Code.

2. This application is for an order pursuant to Section 2518 of Title 18, United States Code, approving the emergency interception of (wire)(oral)(electronic) communications of (list those persons who were known to be targets at the time the emergency authorization was requested) and others as yet unknown (if wire: "to and from the telephone(s) bearing the number(s) _____, subscribed to by _____ and located at/billed

to _____") (if oral: "occurring inside the premises located at _____" or "occurring in and around a (describe the make, color and year of the vehicle) bearing the license plate number _____ and the vehicle identification number _____") (if electronic: "to and from the Internet account _____" or "to and from the facsimile machine attached to the telephone bearing the number subscribed to by _____, and located at _____" or "to the paging device bearing the number _____, and subscribed to by _____) concerning offenses enumerated in Section 2516 of Title 18, United States Code (or any federal felony in the case of electronic communications), that is, offenses involving violations of (list section(s) of the U.S.

Code and describe briefly the applicable offense(s)) that were committed by (list targets) and others as yet unknown.

3. On _____, 2001, at _____ (a.m. or p.m.), pursuant to Section 2518(7) of Title 18, United States Code, the (Attorney General, Deputy Attorney General, or the Associate Attorney General) of the United States specially designated the (name the investigative or law enforcement officer, most likely it will be the Director of the Federal Bureau of Investigation) to determine whether an emergency situation existed. Having received that special designation, the (Director of the FBI; other official) made the determination required by 18 U.S.C. 2518(7) and the FBI commenced interceptions over or within (describe the location or facility) on _____, 2001, at _____ (a.m. or p.m.). Attached to this Application is a Memorandum from the FBI memorializing said special designation of the Director and his subsequent determination in accordance with the requirements of 18 U.S.C. 2518(7).

4. I have discussed all of the circumstances of the above offenses with Special Agent _____ of the (name the investigative agency), who has directed and conducted this investigation and have examined the Affidavit of Special Agent _____, which is attached to this Application and is incorporated herein by reference. Based upon that Affidavit, your applicant states upon information and belief that:

a. there is probable cause to believe that (list the violators) and others as yet unknown have committed violations of (list the offenses - must be enumerated in Section 2516 of Title 18, United States Code, or in the case of electronic communications, a federal felony);

b. there is probable cause to believe that particular (wire)(oral)(electronic) communications of (name the targets) concerning the above-described offenses will be obtained through the interception of (wire)(oral) (electronic) communications. In particular, these (wire) (oral)(electronic) communications would concern the (characterize the types of criminal communications expected to be intercepted). In addition, the communications are expected to constitute admissible evidence of the commission of the above-stated offenses;

c. normal investigative procedures were tried and failed, reasonably appeared to be unlikely to succeed if tried, or were too dangerous to employ, as is described in further detail in the attached Affidavit;

d. there is probable cause to believe that (identify fully the telephone(s)/facility from which, or the premises where, the wire, oral, or electronic communications were intercepted) were being used in connection with the commission of the above-described offenses.

5. The attached Affidavit contains a full and complete statement of facts concerning all previous applications which are known to have been made to any judge of competent jurisdiction for approval of the interception of the oral, wire or electronic communications of any of the same individuals, facilities, or premises specified in this Application. (If there has been no previous electronic surveillance, state: "The applicant is aware of no previous applications made to any judge for authorization to intercept the oral, wire or electronic communications of any of the persons or involving the (facilities) (premises) specified in this application.")

WHEREFORE, your applicant believes that there is probable cause to believe that (name the violators) and others as yet unknown were engaged in the commission of offenses involving (cite to the offenses), that (name the targets) and others yet unknown are using (described the telephone/facility or premises as described above) in connection with the commission of the above-described offenses; and that (wire)(oral)(electronic) communications of (name the targets) and others yet unknown would be intercepted (over the above-described telephone or other facility) and/or (within the above-described premises or the above-described vehicle).

Based on the allegations set forth in this application and on the affidavit of Special Agent _____, attached, the applicant requests this court to issue an order pursuant to the power conferred upon it by Section 2518 of Title 18, United States Code, approving the emergency interception of (wire or electronic communications to and from the above-described facility(ies)) and/or (oral communications from the above-described premises) by the (name the law enforcement agency).

(If interception of wire communications is requested, add:

IT IS REQUESTED FURTHER that the approval given be intended to apply not only to the target telephone number(s) listed above, but to any changed telephone number that may have been subsequently assigned to the same cable, pair, and binding posts utilized by the target telephone(s). (If the telephone is a cellular telephone, the language should state: "the approval given be intended to apply not only to the target telephone number(s) listed above, but to any changed telephone number subsequently assigned to or used by the instrument bearing the same electronic serial number as the target cellular phone.") It is also requested that the approval be intended to apply to background conversations that may have been intercepted in the vicinity of the target telephone(s) while the telephone(s) is off the hook or otherwise in use.)

(If multi-jurisdictional approval for a portable/mobile facility is requested, add:

IT IS REQUESTED FURTHER that in the event that the target facility/vehicle was transferred outside the territorial jurisdiction of this Court, interceptions were permitted to take place in any other jurisdiction within the United States.)

IT IS REQUESTED FURTHER, to avoid prejudice to this criminal investigation, that the Court order the providers of electronic communication service and their agents and employees not to disclose or cause a disclosure of this Court's Order or the request for information, facilities, and assistance by the (investigative agency) or the existence of the investigation to any person other than those of their agents and employees who require this information to accomplish the services requested. In particular, said providers and their agents and employees should be ordered not to make such disclosure to a lessee, telephone subscriber, or any target or participant in the intercepted communications.

IT IS REQUESTED FURTHER that the Court order that its Order, this application, the accompanying affidavit, and any related documents filed with the Court with regard to this matter be sealed until further order of this Court, except that copies of the Order(s), in full or redacted form, may be served on the (name the investigative agency/agencies) and the service provider(s) as necessary to effectuate any order of the Court.

DATED this _____ day of _____, 2___.
(Name and title of the applicant)

_____
(NAME)
Assistant United States Attorney

SUBSCRIBED and SWORN to before me
this _____day of _____, 2_ .

_____
UNITED STATES DISTRICT COURT JUDGE
(District)

Affidavit in Support of Application for Approval of Emergency Interception of Wire, Oral or Electronic Communications Under 18 U.S.C. 2518(7)

UNITED STATES DISTRICT COURT

_____DISTRICT OF_____

IN THE MATTER OF THE APPLICATION	)
OF THE UNITED STATES OF AMERICA FOR	)
AN ORDER AUTHORIZING THE INTERCEPTION	)
OF (WIRE)(ELECTRONIC)(ORAL)	)
COMMUNICATIONS	)
	)

AFFIDAVIT IN SUPPORT OF APPLICATION FOR A COURT ORDER APPROVING EMERGENCY INTERCEPTIONS

INTRODUCTION

_____, being duly sworn, deposes and states as follows:

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI"), United States Department of Justice. I have been so employed by the (name the agency) for the past _____ ( ) years. I have participated in investigations involving (organized crime/drug trafficking/money laundering/terrorism, etc.) activities for the past _____ ( ) years. (Describe present assignment.)

2. I am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code, and am empowered by law to conduct

investigations and to make arrests for offenses enumerated in Section 2516 of Title 18, United States Code.

3. This affidavit is submitted in support of an application for an order approving the emergency interception of (wire)(oral)(electronic) communications occurring (describe the facility or premises to which the application and affidavit are directed).

4. I have participated in the investigation of the above offenses. As a result of my personal participation in this investigation, through interviews with and analysis of reports submitted by other (Special Agents of the _____ and/or other state/local law enforcement personnel), I am familiar with all aspects of this investigation. On the basis of this familiarity, and on the basis of other information which I have reviewed and determined to be reliable, I allege the facts to show that:

a. On _____, 2001, at (a.m. or p.m.), the Director of the FBI, having been specially designated by the (Attorney General, Deputy Attorney General, or the Associate Attorney General) pursuant to 18 U.S.C. § 2518(7), reasonably determined that an emergency situation existed that involved (1) an immediate danger of death or serious physical injury to persons, (2) conspiratorial activities threatening the national security interest, or (3)conspiratorial activities characteristic of organized crime, that required (wire) (oral) (electronic) communications to be intercepted before an order authorizing such interception could, with due diligence, be obtained, and that there were grounds upon which an electronic surveillance order could be entered, authorized the emergency interception of (wire) (oral) (electronic) communications over the telephone bearing the number _____, and/or within the location at _____, or over the computer account _____. (Describe the facility or the location fully.)

b. There is probable cause to believe that (name the violators) have committed violations of (list the offenses - must be ones enumerated in Section 2516 of Title 18, United States Code);

c. there is probable cause to believe that particular (wire) (oral) (electronic) communications of (name the interceptees) concerning the above offenses would be obtained through the

interception of such communications over or within (describe the facility or location).

In particular, these communications were expected to concern the specifics of the above offenses, including (i) the nature, extent and methods of the (describe the illegal activity) business of (name the violators) and others; (ii) the nature, extent and methods of operation of the business of (name the violators) and others; (iii) the identities and roles of accomplices, aiders and abettors, co-conspirators and participants in their illegal activities; (iv) the distribution and transfer of the contraband and money involved in those activities; (v) the existence and location of records; (vi) the location and source of resources used to finance their illegal activities; (vii) the location and disposition of the proceeds from those activities; and (viii) the locations and items used in

furtherance of those activities. In addition, these (wire)(oral)(electronic) communications are expected to constitute admissible evidence of the commission of the above-described offenses.

The statements contained in this affidavit are based in part on information provided by Special Agents of the (name the investigative agency/agencies), on conversations held with detectives and officers from the (identify the local/state police department), on information provided by confidential sources, and on my experience and background as a Special Agent of the _____. Since this affidavit is being submitted for the limited purpose of securing an order approving the emergency interception of (wire)(oral)(electronic) communications, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish the necessary foundation for an order approving the emergency interception of (oral)(wire)(electronic) communications.

PERSONS EXPECTED TO BE INTERCEPTED

Include a short description of each known violator; if appropriate, explain why certain participants in the offenses were not expected to be interceptees.

FACTS AND CIRCUMSTANCES

Provide a discussion of the facts in support of the probable cause statements set forth above. **(Only the facts known to the specially designated official at the time he/she made the determination under 18 U.S.C. 2518(7) that an emergency situation existed should be included in the affidavit.)** If informant information provides a basis for any of the required information, provide adequate qualifying language for each informant. Remember that you must show probable cause 1) that the alleged offenses are being committed; 2) that the named subjects and others unknown were committing them; and 3) that the targeted telephone(s) and/or premises were being used to commit these offenses.

NEED FOR INTERCEPTION

Need for (Wire)(Oral)(Electronic) Interception

Based upon your affiant's training and experience, (as well as the experience of the other (Special Agents of the _____ and/or state/local officers), and based upon all of the facts set forth herein, it is your affiant's belief that the interception of (wire)(oral)(electronic) communications was the only available technique that had a reasonable likelihood of securing the

evidence necessary to prove beyond a reasonable doubt that (name the violators), and others as yet unknown were engaged in the above-described offenses.

Your affiant states that the following investigative procedures, which are usually employed in the investigation of this type of criminal case, were tried and failed, reasonably appeared to be unlikely to succeed if they were tried, or were too dangerous to employ.

ALTERNATIVE INVESTIGATIVE TECHNIQUES

(If the emergency involved immediate danger of death or serious physical injury, the necessity for emergency interception is obvious and concerns more than the loss of evidence that might occur before an order could be obtained. If the emergency involves conspiratorial activities threatening the national security, or characteristic of organized crime, in the absence of an immediate physical threat, the emergency is due to the potential loss of evidence before a court order can be obtained.)

Physical Surveillance

(The following is an example of language that discusses the use of physical surveillance in general; you should also discuss the effectiveness of this, and the following other investigative techniques, as they are applicable to your particular case.)

Physical surveillance had been attempted on numerous occasions during this investigation. Although it has proven valuable in identifying some activities and associates of (list the violators), physical surveillance, if not used in conjunction with other techniques, including electronic surveillance, was of limited value. Physical surveillance has not succeeded in gathering sufficient evidence of the criminal activity under investigation. Physical surveillance of the alleged conspirators has not established conclusively the elements of the violations and has not and most likely would not establish conclusively the identities of various conspirators. In addition, prolonged or regular surveillance of the movements of the suspects would most likely be noticed, causing them to become more cautious in their illegal activities, to flee to avoid further investigation and prosecution, to cause a real threat to the safety of the informant(s) and undercover agent(s), or to otherwise compromise the investigation.

Physical surveillance was also unlikely to establish conclusively the roles of the named conspirators, to identify additional conspirators, or otherwise to provide admissible evidence in regard to this investigation because (discuss any of the following which are applicable to the case):

- the subjects were using counter-surveillance techniques, such as erratic driving behavior, or have evinced that they suspect that law enforcement surveillance is being conducted against them; and/or

- it was not possible to determine the full nature and scope of the aforementioned offenses by the use of physical surveillance; and/or

- the nature of the neighborhood forecloses physical surveillance; (e.g., close-knit community, physical location (cul-de-sac, dead-end, large apartment building), observant neighbors); and/or

- further surveillance would have only served to alert the suspects of the law enforcement interest in their activities and compromise the investigation.

Use of Grand Jury Subpoenas

Based upon your affiant's experience and conversations with Assistant United States Attorney _____, who has experience prosecuting violations of criminal law, your affiant believes that subpoenaing persons believed to be involved in this conspiracy and their associates before a Federal Grand Jury would not be completely successful in achieving the stated goals of this investigation. If any principals of this conspiracy, their co-conspirators and other participants were called to testify before the Grand Jury, they would most likely be uncooperative and invoke their Fifth Amendment privilege not to testify. It would be unwise to seek any kind of immunity for these persons, because the granting of such immunity might foreclose prosecution of the most culpable members of this conspiracy and could not ensure that such immunized witnesses would provide truthful testimony. Additionally, the service of Grand Jury subpoenas upon the principals of the conspiracy or their co-conspirators would only (further) alert them to the existence of this investigation, causing them to become more cautious in their activities, to flee to avoid further investigation or prosecution, to threaten the lives of the informant(s) and the undercover agent(s), or to otherwise compromise the investigation.

(Add specific information regarding any persons who have been subpoenaed before the Grand Jury, especially when the Fifth Amendment was invoked or when the witness later advised the targets.)

Confidential Informants and Cooperating Sources

Reliable confidential informants/cooperating sources have been developed and used in regard to this investigation. However, these sources (discuss only those that are applicable):

- exist on the fringe of this organization and have no direct contact with mid- or high-level members of the organization, or such contact was virtually impossible because the sources had no need to communicate with such individuals; and/or

- refuse to testify before the Grand Jury or at trial because of fear of personal or family safety, or their testimony would be uncorroborated or otherwise would be subject to impeachment (due to prior record, criminal involvement, etc.); and/or

- are no longer associated with the subjects of this investigation (and their information is included for historical purposes only); and/or ·

- are unable to furnish information which would identify fully all members of this ongoing criminal conspiracy or which would define the roles of those conspirators sufficiently for prosecution.

(In addition, discuss whether the information provided by the confidential sources, even if all sources agreed to testify, would not, without the requested electronic surveillance, result in a successful prosecution of all of the participants.)

Undercover Agents

Undercover agents were unable to infiltrate the inner workings of this conspiracy due to the close and secretive nature of this organization. Your affiant believed that there were no undercover agents who could infiltrate the conspiracy at a level high enough to identify all members of the conspiracy or otherwise satisfy all the goals of this investigation. (Indicate if infiltration was not feasible because the confidential informant(s) was not in a position to make introductions of undercover agents to mid- or high-level members of the organization.)

(Details of the use of undercover agents should have been provided in the body of the affidavit, with this section indicating the limitations of such use.)

Interviews of Subjects or Associates

Based upon your affiant's experience, I believe that interviews of the subjects or their known associates would have produced insufficient information as to the identities of all of the persons involved in the conspiracy, the location of documentary evidence and other pertinent information regarding the named crimes. Your affiant also believed that any responses to

the interviews would have contained a significant number of untruths, diverting the investigation with false leads or otherwise frustrating the investigation. Additionally, such interviews would also have the effect of alerting the members of the conspiracy, thereby compromising the investigation and resulting in the possible destruction or concealment of documents and other evidence, and the possibility of harm to cooperating sources whose identities may become known or whose existence may otherwise be compromised.

Search Warrants

The execution of search warrants in this matter has been considered. However, use of such warrants would, in all likelihood, not yield a considerable quantity of evidence nor would the searches have revealed the total scope of the illegal operation and the identities of the co-conspirators. (It is unlikely that all, or even many, of the principals of this organization would be at any one location when a search warrant was executed.) The affiant believed that search warrants executed at this time would be more likely to compromise the investigation by alerting the principals to the investigation and allowing other unidentified members of the conspiracy to insulate themselves further from successful detection.

Pen Registers/Telephone Toll Records/Traps and Traces

Pen register (and/or trap and trace) information has been used in this investigation, including pen register(s) (and/or traps and traces) on the target telephone(s), as described above. The pen register (and/or trap and trace) information has verified frequent telephone communication between the target telephone(s) and other telephones. Pen registers (and/or traps and traces), however, do not record the identity of the parties to the conversation, cannot identify the nature or substance of the conversation, or differentiate between legitimate calls and calls for criminal purposes. A pen register (and/or trap and trace) cannot identify the source or sources of the controlled substances, nor can it, in itself, establish proof of the conspiracy. Telephone toll information, which identifies the existence and length of telephone calls placed from the target telephone to telephones located outside of the local service zone, has the same limitations as pen registers (and/or traps and traces), does not show local calls, and is generally available only on a monthly basis.

Other Limitations

Focus here on the nature of the emergency situation and the need to act quickly.

Based upon the foregoing, it is your affiant's belief that the emergency interception of (wire)(oral)(electronic) communications was an essential investigative means in obtaining evidence of the offenses in which the subject(s) and others as yet unknown were involved.

PRIOR APPLICATIONS

Based upon a check of the records of the (Federal Bureau of Investigation, the Drug Enforcement Administration, and any other appropriate agency), no prior federal applications for an order authorizing or approving the interception of wire, oral, or electronic communications have been made involving the persons, premises or facilities named herein. (If the facts warrant, include additional information concerning prior or ongoing electronic surveillance, including the dates of the interception, the jurisdiction where the order was signed and the relevance, if any, to the instant application. While there is no obligation to conduct a search of state law enforcement electronic surveillance indices, information about prior state taps must be included if the government has knowledge of them through other means.)

MINIMIZATION

All interceptions were minimized in accordance with the minimization requirements of Chapter 119 of Title 18, United States Code. (Indicate here whether the interceptions have been terminated or whether you plan to seek an extension of the interceptions for a thirty-day period.)

_____

(NAME)

Special Agent

(Agency)

Sworn to before me this
_____ day of _____, 2___.

_____
UNITED STATES DISTRICT COURT JUDGE
(District)

Order Approving Emergency Interception of Wire, Oral or Electronic Communications Under 18 U.S.C. 2518(7)

UNITED STATES DISTRICT COURT

_____ DISTRICT _____

IN THE MATTER OF THE APPLICATION	)
OF THE UNITED STATES OF AMERICA FOR	)
AN ORDER APPROVING THE EMERGENCY	)
INTERCEPTION OF (WIRE)(ORAL)	)
(ELECTRONIC) COMMUNICATIONS	)
	)

ORDER APPROVING THE EMERGENCY INTERCEPTION OF (WIRE) (ORAL)(ELECTRONIC) COMMUNICATIONS

Application under oath having been made before me by _____, Assistant United States Attorney, _____ District of _____, an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code, for an Order approving the emergency interception of (wire) (oral)(electronic) communications pursuant to Section 2518 of Title 18, United States Code, and full consideration having been given to the matter set forth therein, the Court finds:

a. there is probable cause to believe that (list the targets) have committed violations of (list the offenses - must be ones enumerated in Section 2516 of Title 18, United States Code, or in the case of electronic communications, a federal felony);

b. there is probable cause to believe that particular (wire)(oral)(electronic) communications of (name the targets) concerning the above-described offenses would be obtained through

the emergency interception for which the (name the law enforcement official) was specially designated by the (Attorney General, Deputy Attorney General, Associate Attorney) of the United States to conduct. In particular, there is probable cause to believe that the interception of (wire communications to and from the telephone bearing the number _____, subscribed to by _____ and located at/billed to _____) (oral communications occurring in the premises located at _____ and/or in and around the vehicle described as _____) (electronic communications to the pager bearing the number _____, and subscribed to by _____, or Internet account _____, or facsimile machine attached to the telephone bearing the number _____, subscribed to by _____, and located at _____), would concern the specifics of the above offenses, including the manner and means of the commission of the offenses(s);

c. it has been established that normal investigative procedures were tried and failed, reasonably appeared to be unlikely to succeed if tried, or were too dangerous to employ; and

d. there is probable cause to believe that (identify the facilities from which, or the place where, the wire, electronic or oral communications were to be intercepted) have been used in connection with commission of the above-described offenses.

WHEREFORE, IT IS HEREBY ORDERED that Special Agents of the (name the investigative agency/agencies; also indicate if state and local officers were participating in the investigation, particularly if they were monitors) were authorized, pursuant to 18 U.S.C. 2518(7), to conduct emergency interceptions, there being an emergency situation that involved (one or more of the following: 1) an immediate danger of death or serious physical injury to any person, 2) conspiratorial activities threatening the national security interest, or 3) conspiratorial activities characteristic of organized crime), and that a court order could not, with due diligence, be obtained before interceptions could begin.

IT IS ORDERED FURTHER that in the event that the target facility/vehicle was transferred outside the territorial jurisdiction of this court, interceptions were permissible within any other jurisdiction within the United States.)

IT IS ORDERED FURTHER that the approval apply not only to the target telephone number(s) listed above, but to any changed telephone number subsequently assigned to the same cable, pair, and binding posts utilized by the target telephone(s). (In the case of a cellular telephone: "... but to any changed telephone number or any other telephone number subsequently assigned to or used by the instrument bearing the same electronic serial number as the target cellular phone") It is also ordered that the approval apply to background conversations intercepted in the vicinity of the target telephone(s) while the telephone(s) was off the hook or otherwise in use.)

IT IS ORDERED FURTHER that, to avoid prejudice to the government's criminal investigation, the provider(s) of the electronic communications service and its agents and employees are ordered not to disclose or cause a disclosure of the Order or the request for information, facilities and assistance by the (investigative agency), or the existence of the investigation to any person other than those of its agents and employees who require this information to accomplish the services hereby ordered. In particular, said provider(s) and its agents and employees shall not make such disclosure to a lessee, telephone subscriber or any target or participant in the intercepted communications.

IT IS ORDERED FURTHER that this Order, the application, affidavit and proposed order(s), and all interim reports filed with this Court with regard to this matter, shall be sealed until further order of this Court, except that copies of the order(s), in full or redacted form, may be served on the (investigative agency/agencies) and the service provider(s) as necessary to effectuate this order.

_____

UNITED STATES DISTRICT COURT JUDGE

(District)

Dated this _____ day of _____, 2___.

Application for Sealing

UNITED STATES DISTRICT COURT

_____ DISTRICT OF _____

_____

IN THE MATTER OF THE APPLICATION)
OF THE UNITED STATES OF AMERICA)
FOR AN ORDER AUTHORIZING (APPROVING))
The INTERCEPTION OF (WIRE)(ORAL))
(ELECTRONIC) COMMUNICATIONS OCCURRING)
TO AND FROM (TELEPHONE NUMBER _____)
SUBSCRIBED TO BY _____)
_____.) (THE PREMISES KNOWN)
AS _____, LOCATED AT _____)
_____.) (THE FACSIMILE)
MACHINE/PAGER BEARING NUMBER _____)
_____ AND SUBSCRIBED TO BY _____)
_____.))
_____)

SEALING APPLICATION

The UNITED STATES OF AMERICA, by Assistant United States Attorney _____, herein applies for an Order:

(a) Sealing _____ (reel-to-reel, cassette, computer printouts, magneto optical disk, etc.) recordings of (wire, oral and/or electronic) communications intercepted between _____ and _____, pursuant to the Order of this Court dated _____, (occurring to and from (telephone number _____ subscribed to by _____ and located at/billed to _____) (the premises known as _____ and located at _____);

(b) Directing that the aforementioned recordings be held in the custody of the (name the investigative agency, e.g. Federal Bureau of Investigation) for a period of ten (10) years from the

date of this Order in a manner so as to prevent editing, alteration and/or destruction;

(c) Directing that the contents of the said recordings be disclosed only upon the order of this Court or any other Court of competent jurisdiction, except as otherwise authorized by Title 18, United States Code, Section 2517;

(d) Postponing the notification requirements of Title 18, United States Code, Section 2518(d) as to all parties intercepted during the subject electronic surveillance until further order of this Court; and

(e) Directing that this Order and Application be sealed until further order of this Court.

In support of the Application, the UNITED STATES OF AMERICA represents as follows:

1. On _____, the (name the investigative agency) applied for an Order from this Court authorizing the interception of (wire)(oral)(electronic) communications occurring to and from (telephone number, subscribed to by _____)(the premises known as _____, and located at _____). The application for authorization to intercept communications (over said telephone number)(at said premises) was supported by probable cause to believe that (name the subjects) and others have been and are committing offenses involving the importation, possession with intent to distribute and distribution of narcotic drug controlled substances, conspiracy to do the same, attempts to do the same, and use of wire facilities to facilitate the same, in violation of Sections _____, Title _____, United States Code; and that evidence of said violations would be obtained through the interception of the subject (wire)(oral)(electronic) communications.

2. The requested Order was granted on _____, and authorized electronic surveillance (over the subject telephone/facsimile machine/pager)(at the subject premises) for a period of thirty (30) days. Surveillance began on _____, and continued until _____.

3. The investigation of the named subjects, as well as others who are believed to be associated with the subjects is continuing. Accordingly, notification to the parties whose

communications were intercepted would alert the subjects to the existence and extent of the investigation.

WHEREFORE, I respectfully request that the Court issue an Order granting this Application.

_____

Assistant United States Attorney

Order for Sealing

UNITED STATES DISTRICT COURT

_____ DISTRICT OF _____

_____

IN THE MATTER OF THE APPLICATION)
OF THE UNITED STATES OF AMERICA)
FOR AN ORDER AUTHORIZING (APPROVING))
THE INTERCEPTION OF (WIRE COMMUNICATIONS)
OCCURRING TO AND FROM TELEPHONE NUMBER)
_____ SUBSCRIBED TO BY)
_____) (ORAL)
COMMUNICATIONS WITHIN THE PREMISES KNOWN)
AS _____, LOCATED AT _____)
_____.) (ELECTRONIC COMMUNICA-)
TIONS OVER THE FACSIMILE MACHINE/PAGER)
BEARING NUMBER _____ AND SUBSCRIBED)
TO BY _____.))
_____)

ORDER

Upon consideration of the attached application of the UNITED STATES OF AMERICA, by Assistant United States Attorney _____ _____, and upon finding that disclosure of the subject electronic surveillance would interfere with an ongoing criminal investigation, and also upon finding that the motion of the UNITED STATES OF AMERICA is made in good faith, it is hereby:

ORDERED

1. That ____ (reel-to-reel, cassette, magneto optical disk, computer printouts) recordings of (wire)(oral)(electronic) communications intercepted between _____ and _____, pursuant to the Order of this Court dated _____, (occurring to and from the telephone number _____, subscribed to by _____) (within the premises known as

_____, and located at _____) be sealed;

2. That the aforementioned recordings be held in the custody of the (name the investigative agency) for a period of ten (10) years from the date of this Order in a manner so as to prevent editing, alteration and/or destruction;

3. That the contents of the said recordings be disclosed only upon the order of this Court or any other Court of competent jurisdiction, except as otherwise authorized by Title 18, United States Code, Section 2517;

4. That the notification requirements to Title 18, United States Code, Section 2518(d) be postponed as to all parties intercepted during the subject electronic surveillance until further order of this Court; and

5. That this Order and Application be sealed until further order of this Court.

_____

UNITED STATES DISTRICT COURT JUDGE

(District)

Application for 2703(d) Court Order

UNITED STATES DISTRICT COURT

_____ DISTRICT OF _____

_____

IN THE MATTER OF THE APPLICATION)
OF THE UNITED STATES OF AMERICA)
FOR AN ORDER PURSUANT TO 18 U.S.C.)
2703(d)_____)
_____)

APPLICATION

_____, an Assistant United States Attorney for the _____ District of _____, hereby applies to the court for an order, pursuant to 18 U.S.C. 2703(d), directing (provider of electronic communication service or remote computing service) to disclose the (**choose as appropriate**: name; address; local and long distance telephone connection records, or records of session times and durations; length of service [including start date] and types of service utilized; telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; means and source of payment for such service [including any credit card or bank account number]; cell site information) of a subscriber to or customer of such service. In support of this application, I state the following:

I am an attorney for the Government as defined in Rule 1(b)(1) of the Federal Rules of Criminal Procedure and, therefore, pursuant to Section 2703© of Title 18, United States Code, may apply for an order as requested herein.

I certify that the (investigative agency) is conducting a criminal investigation in connection with possible violation(s) of (list principal violations); that it is believed that the subjects of the investigation are using the (**choose as appropriate**: telephone or instrument number; other subscriber number or identity; temporarily assigned network address) in furtherance of the subject offenses; and that the information sought is relevant and material to an ongoing criminal investigation. (Offer

specific and articulable facts showing that there are reasonable grounds for such belief.)

Wherefore, the applicant requests that the Court issue an order pursuant to 18 U.S.C. 2703(d) directing (provider of electronic communication service or remote computing service) to provide the requested information forthwith.

I request further that this Court's order delay notification of this application and this order to the subscriber or customer for a period not to exceed ninety days, and that the Court command the provider of electronic communication service or remote computing service not to notify any other person of the existence of this application and this order (for such period as the court deems appropriate) because such notification would seriously jeopardize the investigation.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on _____, 20___

_____

Applicant Signature

_____

Title

2703(d) Court Order

UNITED STATES DISTRICT COURT

_____ DISTRICT OF _____

_____

_____

IN THE MATTER OF THE APPLICATION)
OF THE UNITED STATES OF AMERICA)
FOR AN ORDER PURSUANT TO 18 U.S.C.)
2703(d))
_____)

ORDER

This matter having come before the court pursuant to an application under Title 18, United States Code, Section 2703© by _____, an attorney for the Government, which application requests an order under Title 18, United States Code, Section 2703(d) directing (provider of electronic communication service or remote computing service) to disclose the (**choose as appropriate**: name; address; local and long distance telephone connection records, or records of session times and durations; length of service [including start date] and types of service utilized; telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; means and source of payment for such service [including any credit card or bank account number]; cell site information) of a subscriber to or customer of such service, and the Court finds that the applicant has offered specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation, and

IT APPEARING that the information sought is relevant and material to an ongoing criminal investigation, and that disclosure to any person of this investigation or this application and order entered in connection therewith would seriously jeopardize the investigation;

IT IS ORDERED pursuant to Title 18, United States Code, Section 2703(d) that (provider of electronic communication service or remote computing service) will, forthwith, turn over to agents

of the (investigative agency) the (name; address; local and long distance telephone connection records, or records of session times and durations; length of service [including start date] and types of service utilized; telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; means and source of payment for such service [including any credit card or bank account number]) of (subscriber to or customer of such service).

IT IS FURTHER ORDERED that the application and this order are sealed until otherwise ordered by the court; that the government may delay notice of this order to the subscriber or customer for a period not to exceed ninety days; and that (provider of electronic communication service or remote computing service) is commanded not to notify any other person of the existence of this application and order (for such period as the court deems appropriate), the court having determined that there is reason to believe that such notifications would seriously jeopardize the investigation.

DATED: _____

_____

UNITED STATES MAGISTRATE (or DISTRICT) JUDGE

Application for Trap and Trace/Pen Register

UNITED STATES DISTRICT COURT

_____ DISTRICT OF _____

IN THE MATTER OF THE	)
APPLICATION OF THE	)
UNITED STATES OF AMERICA	)
FOR AN ORDER AUTHORIZING	)
THE INSTALLATION AND USE	)
OF A (PEN REGISTER)	)
(TRAP AND TRACE DEVICE)	)
	)

APPLICATION

_____, an Assistant United States Attorney, being duly sworn, hereby applies to the Court for an order authorizing the installation and use of a (pen register) (trap and trace device) on (telephone line _____ or other facility). In support of this application I state the following:

1. Applicant is an "attorney for the Government" as defined in Rule 1(b)(1) of the Federal Rules of Criminal Procedure, and, therefore, pursuant to Section 3122 of Title 18, United States Code, may apply for an order authorizing the installation of a (trap and trace device) (pen register).

2. Applicant certifies that the (investigative agency) is conducting a criminal investigation of (name targets) and others as yet unknown, in connection with possible violations of (list violations); it is believed that the subjects of the investigation are using (telephone line _____ or other facility), (listed in the name of _(if known)_or leased to _(if known)_ and located at ___(if known)__ in furtherance of the subject offenses; and that the information likely to be obtained from the (pen register) (trap and trace device) is relevant to the ongoing criminal investigation in that it is believed that this information will concern the aforementioned offenses.

3. Applicant requests that the Court issue an order authorizing the installation and use of (a pen register to record or decode dialing, routing, addressing, or signaling information transmitted by [identify the targeted instrument or facility from which a wire or electronic communication is transmitted]), (and) (a trap and trace device to capture the incoming electronic or

other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication), for a period of (enter time period, not to exceed 60) days, provided, however, that such information shall not include the contents of any communication.

4. The applicant requests further that the order direct the furnishing of information, facilities, and technical assistance necessary to accomplish the installation of (the pen register) (and/or) (trap and trace device) as provided in Section 3124 of Title 18.

5. (If trap and trace requested) The applicant requests further that the order direct that the results of the trap and trace device be furnished to the officer of a law enforcement agency, designated in the court order, at reasonable intervals during regular business hours for the duration of the order.

6. With regard to the requirement of Section 3121(c) of Title 18 that the (investigative agency) use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing, routing, addressing, and signaling information utilized in the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications, the (investigative agency) is not aware of any such technology.

WHEREFORE, it is respectfully requested that the Court grant an order for (enter time period, not to exceed 60) days authorizing the installation and use of (a pen register) (trap and trace device), and directing the (communications service provider) to forthwith furnish agents of the (investigative agency) with all information, facilities and technical assistance necessary to accomplish the installation of the (trap and trace device) (pen register).

I declare under penalty of perjury that he foregoing is true and correct.

EXECUTED ON _____, 20____

_____

Applicant

Order for Trap and Trace/Pen Register

UNITED STATES DISTRICT COURT
_____ DISTRICT OF _____

IN THE MATTER OF THE	)
APPLICATION OF THE	)
UNITED STATES OF AMERICA	)
FOR AN ORDER AUTHORIZING	)
THE INSTALLATION AND USE	)
OF A (PEN REGISTER)	)
(TRAP AND TRACE DEVICE)	)
	)

ORDER

This matter having come before the Court pursuant to an application under oath pursuant to Title 18, United States Code, Section 3122 by _____, an attorney for the Government, which requests an order under Title 18, United States Code, Section 3123, authorizing the installation and use of a (pen register) on (telephone line _____ or other facility), the Court finds that the applicant has certified that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation into possible violations of (list violations) by (list targets, if known), and others as yet unknown.

IT APPEARING that the information likely to be obtained by a (pen register) (trap and trace device) installed on (telephone line_____or other facility), (listed in the name of __ (if known)) (leased to__(if known)__), (and located at __(if known)___), is relevant to an ongoing criminal investigation of the specified offenses,

IT FURTHER APPEARING that [conform to application statement] with regard to the limitation in Section 3121© of Title 18 concerning pen register technology, the (investigative agency) does not have technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing, routing, addressing, and signaling information utilized in the processing and transmitting of wire or electronic

communications so as not to include the contents of any wire or electronic communications.

IT IS ORDERED, pursuant to Title 18, United States Code, Section 3123, that (investigative agency) is authorized to install and use, anywhere within the United States, on (telephone line ____ or other facility) (a pen register to record or decode dialing, routing, addressing, or signaling information) (and) (a trap and trace device to capture the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication) for a period of (enter time period, not to exceed 60) days; and

IT IS ORDERED FURTHER, pursuant to Section 3123(b)(2) of Title 18, that upon the request of (attorney for the Government or an officer of the law enforcement agency authorized to install and use the pen register), (provider of wire or electronic communication service, landlord, custodian, or other person) shall furnish such (investigative or law enforcement officer) forthwith all information, facilities, and technical assistance necessary to accomplish the installation of the pen register unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place, (and) (if trap and trace ordered) that upon the request of (attorney for the Government or officer of the investigative agency authorized to receive the results of the trap and trace device), (provider of a wire or electronic communication service, landlord, custodian, or other person) shall install such device forthwith on the appropriate line or other facility and shall furnish (investigative or law enforcement officer) all additional information, facilities and technical assistance including installation and operation of the device (including the installation of Caller ID service on telephone line _____ or other facility) unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place. The results of the trap and trace device shall be furnished to the (officer of a law enforcement agency, designated in the court order), at reasonable intervals during regular business hours for the duration of the order.

IT IS ORDERED FURTHER that the (investigative agency) will reasonably compensate the provider of a wire or electronic communication service, landlord, custodian, or other person who furnishes facilities or technical assistance for such reasonable expenses incurred in providing such facilities and assistance in complying with this order.

IT IS ORDERED FURTHER, pursuant to Section 3123(d) of Title 18, that this order and the application be sealed until otherwise ordered by the Court, and that the person owning or leasing the

line or other facility to which the pen register or a trap and trace device is attached or applied, or who is obligated by the order to provide assistance to the applicant, not disclose the

existence of the (pen register) (trap and trace device), or the existence of the investigation to the listed subscriber, or to any other person, unless or until otherwise ordered by the Court.

_____

UNITED STATES MAGISTRATE (or DISTRICT) JUDGE

_____ Date

Application for Order Permitting Government To Use Its Own Pen Register/Trap and Trace Equipment (Triggerfish/Digital Analyzer or Similar Device)

UNITED STATES DISTRICT COURT

_____ DISTRICT OF _____

IN THE MATTER OF THE	)
APPLICATION OF THE	)
UNITED STATES OF AMERICA	)
FOR AN ORDER AUTHORIZING	)
THE INSTALLATION AND USE	)
OF A PEN REGISTER	)
	)

APPLICATION

_____, an Assistant United States Attorney, being duly sworn, hereby applies to the Court for an order authorizing the installation and use of a pen register to identify the Electronic Serial Number (ESN) and Mobile Identification Number (MIN) of a cellular telephone (being used by _(if known)_) (within a (color, make, model of vehicle) (bearing ____ state license plate number ____)). In support of this application I state the following:

1. Applicant is an "attorney for the Government" as defined in Rule 1(b)(1) of the Federal Rules of Criminal Procedure, and, therefore, pursuant to Section 3122 of Title 18, United States Code, may apply for an order authorizing the installation of a trap and trace device and pen register.

2. Applicant certifies that the United States Drug Enforcement Administration is conducting a criminal investigation of (name targets (if known) and others as yet unknown), in connection with possible violations of Title __, United States Code, Section(s)____; it is believed that the subjects of the investigation are using a cellular telephone within a (color, make, model of vehicle) (bearing ____ state license plate number ____)) in furtherance of the subject offenses; and that the information likely to be obtained from the pen register is relevant to the ongoing criminal investigation.

3. Applicant requests that the Court issue an order authorizing the installation and use of a pen register for a period of (enter time period, not to exceed 60) days.

WHEREFORE, it is respectfully requested that the Court grant an order for (enter time period, not to exceed 60) days authorizing the installation and use of a pen register.

I declare under penalty of perjury that he foregoing is true and correct.

EXECUTED ON _____, 20____

_____

Applicant

Order Permitting Government To Use Its Own Pen Register/Trap and Trace Equipment (Triggerfish/Digital Analyzer or Similar Device)

UNITED STATES DISTRICT COURT

_____ DISTRICT OF _____

IN THE MATTER OF THE	)
APPLICATION OF THE	)
UNITED STATES OF AMERICA	)
FOR AN ORDER AUTHORIZING	)
THE INSTALLATION AND USE	)
OF A PEN REGISTER	)
	)

ORDER

This matter having come before the Court by an application under oath pursuant to Title 18, United States Code, Section 3122 by _____, an attorney for the Government, which requests an order under Title 18, United States Code, Section 3123, authorizing the installation and use of a pen register to identify the Electronic Serial Number (ESN) and Mobile Identification Number (MIN) assigned to a cellular telephone (being used by __(if known)__) (within a (color, make, model of vehicle), bearing (____ state license plate number ____)), the Court finds that the applicant has certified to the Court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation into possible violations of Title __, United States Code, Sections ____ by (list targets (if known) and others as yet unknown).

IT IS ORDERED, pursuant to Title 18, United States Code, Section 3123, that the (investigative agency) is authorized to install and use, anywhere within the United States, a pen register to identify the ESN and MIN of a cellular telephone (being used by __(if known)__) (within a (color, make, model of vehicle), bearing (____ state license plate number ____)), for a period of (enter time period, not to exceed 60) days; and

IT IS ORDERED FURTHER, pursuant to Section 3123(d) of Title 18, that this order and the application be sealed until otherwise ordered by the Court.

_____

UNITED STATES MAGISTRATE (or DISTRICT) JUDGE

_____ Date

Combined 3123/2703 Application

[NAME]
United States Attorney
[NAME]
Special Assistant United States Attorney
Chief, Criminal Division
[YOUR NAME]
Assistant United States Attorney
[_____] Section
State Bar No. **[_____]**
[ADDRESS]
[CITY STATE ZIP
Telephone: (XXX) -**[____]**
Facsimile: (XXX) -**[____]**

Attorneys for Applicant
United States of America

UNITED STATES DISTRICT COURT

FOR THE [XXXX] DISTRICT OF [STATE]

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER: (1) AUTHORIZING THE INSTALLATION AND USE OF A PEN REGISTER AND A TRAP AND TRACE DEVICE AND (2) AUTHORIZING RELEASE OF SUBSCRIBER INFORMATION, AND CELL SITE INFORMATION _____	No. _____ **[NOTE: IF CONTINUATION OF EXISTING PEN REGISTER ORDER, INSERT THE ORIGINAL MISC. NO. ABOVE, FOLLOWED BY (A), (B) ETC. FOR EACH SUCCESSIVE CONTINUATION; ALSO INDICATE "FIRST EXTENSION," "SECOND EXTENSION", ETC. UNDER "APPLICATION"; IF AMENDED OR SUPPLEMENTAL APPLICATION, STATE SAME]** A P P L I C A T I O N (UNDER SEAL)

A. INTRODUCTION

[**YOUR NAME**], an Assistant United States Attorney for the Central District of California, hereby applies to the court for an order: **[NOTE: FOR CONTINUATION OF EXISTING ORDER, REPLACE "INSTALLATION AND USE" WITH "CONTINUED USE" THROUGHOUT THIS APPLICATION AND ORDER]**

1. Pursuant to 18 U.S.C. §§ 3122 and 3123, authorizing the **[installation and] [continued]** use of a pen register and trap and trace device[33] on the following telephone number**[s]**:[34] **[NOTE: WHEN IT IS AVAILABLE, HAVE AGENTS SHOW YOU THE FAX FROM TELEPHONE COMPANY CONTAINING SUBJECT TELEPHONE AND SUBSCRIBER INFORMATION AND MAKE SURE INFORMATION MATCHES; ALSO, TRY TO HAVE AGENTS CONFIRM THAT TELEPHONE INFORMATION IS CURRENT WITHIN 48 HOURS BECAUSE PENS ARE SO EXPENSIVE]**

(a) **[AREA CODE AND TELEPHONE NUMBER; AVOID USING "UFMI," WHICH RELATES TO NEXTEL'S "DIRECT CONNECT" WALKIE-TALKIE FEATURE, AS YOUR SUBJECT TELEPHONE NUMBER UNLESS YOU CANNOT GET TELEPHONE NUMBER FOR REASONS STATED IN FOOTNOTE BELOW; IF MUST USE UFMI, INSERT FOOTNOTE AS FOLLOWS [35]**, a **[TYPE OF**

---

[33] A "pen register" is a "device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication . . ." 18 U.S.C. § 3127(3). A "trap and trace device" is "a device or process which captures the incoming electronic or other impulses which identify the originating number" or other identifiers "reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information not include the contents of any communication. 18 U.S.C. § 3127(4).

[34] Section 3123, as amended (P.L. 107-56 (2001)), empowers courts to authorize the installation and use of pen registers and trap and trace devices in other districts. Section 3123(a)(1) provides that the court may enter an order authorizing a pen register or trap and trace device "anywhere within the United States. . . ." Moreover, Section 3127(2)(A) now defines a "court of competent jurisdiction" as "any district court of the United States (including a magistrate judge of such a court)
. . . having jurisdiction over the offense being investigated." 18 U.S.C. § 3127(2)(A).

[35] [UFMI is an acronym for "Urban Fleet Mobile Identifier." The UFMI is the unique telephone number associated with Nextel's "Direct Connect"/"Direct Dispatch" walkie-talkie feature. Nextel cellular telephones with the walkie-talkie feature thus have two identifiable telephone numbers: the mobile identification number (MIN, frequently referred to as the public telephone number) and

TELEPHONE, e.g., "cellular"; if prepaid, state "prepaid cellular"] issued by **[NAME OF CARRIER, e.g., Verizon Wireless]**, with Electronic Serial Number ("ESN")[36] **[INSERT ESN]** [**If T-Mobile or Nextel telephones: instead of ESN, insert International Mobile Subscriber Identity ("IMSI"), and/or International Mobile station Equipment Identity ("IMEI")**[37]]; **[if Cingular Wireless, insert ESN and/or Subscriber Identity Module ("SIM")**[38]] subscribed to by [**SUBSCRIBER'S NAME AND ADDRESS**]; **[NOTE: IF SUBSCRIBER NAME AND ADDRESS IS UNKNOWN BECAUSE SUBJECT TELEPHONE IS PREPAID, THEN INSERT FOOTNOTE AS FOLLOWS [**[39]**]] [IF SUBSCRIBER NAME AND**

---

the UFMI. Like a pen register or trap and trace on the public telephone number, a pen register or trap and trace on the UFMI will not disclose content of the call. The [AGENCY/IES] obtained the UFMI from a [confidential source] [criminal associate]. Due to the immediate need to locate the fugitive target before he/she stops using the **Subject Telephone Number[s]**, there is insufficient time to obtain the corresponding MIN (public telephone number) from the subject telephone company, which could take up to several weeks, without jeopardizing the fugitive investigation.]

[36] ESN is an acronym for "Electronic Serial Number." The ESN uniquely identifies cellular telephone instruments.

[37] IMSI is an acronym for "International Mobile Subscriber Identity." Every mobile phone that uses GSM format has a SIM (Subscriber Identity Module) card that is installed or inserted into the mobile phone handset. The SIM card contains the IMSI, which is a non-dialable number programmed on a microchip on the SIM card. It is the IMSI that is used to uniquely identify a subscriber to the GSM mobile phone network. The IMSI number is unique to that SIM card and is never re-assigned. Thus, if the target exchanges his cell phone for an updated model and/or changes his phone number, but retains his SIM card, the IMSI will remain the same. The IMEI (International Mobile station Equipment Identity) is similar to a serial number and uniquely identifies the telephone handset itself.

[38] SIM is an acronym for "Subscriber Identity Module." The SIM is a card, sometimes called a "smart" card, which can be installed or inserted into certain cellular telephones containing all subscriber-related data. This facilitates a telephone call from any valid cellular telephone since the subscriber data is used to complete the call rather than the telephone's internal serial number.

[39] [Subscriber information for the **Subject Telephone Number[s]** is not known because telephone companies do not require the

ADDRESS IS UNKNOWN BECAUSE IT IS A FUGITIVE INVESTIGATION AND THERE WAS NO TIME TO GET SUBSCRIBER INFORMATION, THEN INSERT FOOTNOTE AS FOLLOWS [[40]]] and believed to be used by [**TARGET'S NAME**] (hereinafter the "**Subject Telephone Number**") [**NOTE: For other carriers, check with your agent to determine whether it is MIN/ESN, IMSI/IMEI or SIM]**

(b) **[REPEAT ABOVE FOR EACH ADDITIONAL SUBJECT PHONE. IF REQUESTING PEN ON MULTIPLE PHONES, OR YOU PLAN TO REQUEST PENS ON FUTURE PHONES IN THE SAME CASE, THEN NUMBER PHONES AS FOLLOWS: "Subject Telephone Number One," "Subject Telephone Number Two," etc.]**

[NOTE: IF REQUESTING PEN ON MORE THAN ONE SUBJECT TELEPHONE, BE SURE TO USE PLURAL "SUBJECT TELEPHONE NUMBERS" THROUGHOUT APPLICATION AND ORDER!! JUST SEARCH FOR BRACKETS AND REVISE AS APPROPRIATE]**

2. Pursuant to 18 U.S.C. §§ 2703© and 2703(d), directing the electronic service providers to disclose or provide upon oral or written request by Special Agents of the **[AGENCY/IES]**:

a. Records or other information identifying subscribers or customers (but not including the contents of communications or toll records), namely, subscriber name, address, date of birth, social security number, driver's license (state and number), contact names and numbers, employment information, method of payment, length of service, and type of service utilized, for all published, non-published, listed, or unlisted numbers, dialed or otherwise transmitted to and from the **Subject Telephone Number[s]**;

b. All changes (including additions, deletions, and transfers) in service regarding the **Subject Telephone Number[s]** to include telephone numbers and subscriber information (published, non-published, listed, or unlisted) associated with these service changes; [and]

c. For the **Subject Telephone Number[s]**, records or other information pertaining to subscriber(s) or customer(s), including historical cellsite information[41] and call detail records[42]

---

subscriber to provide identification when purchasing a prepaid cellular telephone because the fees are paid in advance.]

[40] [AGENCY/IES] obtained the **Subject Telephone Number[s]** from a [confidential source] [criminal associate]. Due to the immediate need to locate the fugitive target before he/she stops using the **Subject Telephone Number[s]**, there is insufficient time to obtain subscriber records from the telephone company, which could take up to several weeks, without jeopardizing the fugitive investigation.]

[41]A cellsite is located in a geographic area within which wireless service is supported through radio signaling to and from antenna tower(s) operated by a service provider. Cellsites are located throughout the United States. Cellular telephones that are powered on will automatically register or re-register with a cellular tower as the phone travels within the provider's service area. The

[including direct connect records[43]] for the following dates: _____ to the present **[THE LAST TEN DAYS IS RECOMMENDED]** (but not including the contents of communications).

d. For the **Subject Telephone Number[s]**, all cellsite information provided to the government on a continuous basis contemporaneous with call origination (for outbound calling) and call termination (for incoming calls), and at such other time upon the oral or written request of the government, including if reasonably available, during the progress of a call. Specific disclosure of cellsite information will assist law enforcement in identifying the approximate physical location of the **Subject Telephone** and will not disclose content of the calls.

II. CERTIFICATION FOR A PEN REGISTER AND A TRAP AND TRACE DEVICE PURSUANT TO 18 U.S.C. §§ 3122 AND 3123

In support of this application, I state the following:

1. I am an "attorney for the Government" as defined in Rule 1(b)(1) of the Federal Rules of Criminal Procedure, and therefore, pursuant to 18 U.S.C. § 3122, may apply for an order

---

registration process is the technical means by which the network identifies the subscriber, validates the account and determines where to route call traffic. This exchange occurs on a dedicated control channel that is clearly separate from that used for call content (i.e. audio)--which occurs on a separate dedicated channel. As used herein, "Cellsite information" refers categorically to any and all data associated with registration of the Subject Telephone with cellsites/network, as well as other data used by the network to establish a connection with the telephone handset and to maintain connectivity to the network. This includes the physical location and/or address of the cellular tower, cellsite sector, control channel number, neighbor cell lists, and any identification numbers, processing data, and parameters not pertaining to the contents of a call.

[42] "Call detail records" are similar to toll records (i.e. historical telephone records of telephone activity, usually listing outgoing calls and date, time, and duration of each call), which are made and retained in the ordinary course of business. However, "call detail records" is the term used when referring to toll records of cellular telephones rather than hardline telephones. Unlike toll records, however, call detail records also include a record of incoming calls and the cell site/sector(s) used by the cellular telephone to obtain service for a call or when in an idle state.

[43] **ASK TECH AGENT: DEFINE DIRECT CONNECT. OR BETTER YET, IS THERE A GENERIC TERM, SUCH AS WALKIE TALKIE FEATURE OR TWO WAY RADIO FEATURE??**

authorizing the installation and use of pen registers and trap and trace devices.

2. I certify that the information likely to be obtained from the pen register and trap and trace devices on the **Subject Telephone Number[s]** is relevant to an ongoing criminal **[fugitive]** investigation being conducted by the **[AGENCY/IES]** in connection with possible violations of federal criminal statutes, including **[CITE VIOLATION(S) AND STATUTE(S), I.E. NARCOTICS DISTRIBUTION IN VIOLATION OF 21 U.S.C. § 841(A)(1)]** by **[LIST MAIN TARGET(S) OR STATE "UNKNOWN INDIVIDUALS"]**.

3. Therefore, based upon the above Certification,[44] and pursuant to 18 U.S.C. §§ 3122 and 3123, I request that the court issue an order authorizing:

a. The **[name agency] to install, or cause the provider to install, and use [continued use]**a pen register device(s) anywhere in the United States to record or decode dialing, routing, addressing, or signaling information (including "post-cut-through dialed digits"[45]) transmitted **[[46]][NOTE: SINCE NEXTEL**

---

[44] Section 3122 "was not intended to require independent judicial review of relevance; rather, the reviewing court need only verify the completeness of the certification." In re United States, 10 F.3d 931, 935 (2d Cir. 1993) (citing S. Rep. No. 541, 99th Cong., 2d Sess. 47 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3601); see also United States v. Fregoso, 60 F.3d 1314, 1320 (8th Cir. 1995) (holding that the judicial role under Section 3123(a) is ministerial in nature because a proper application under Section 3122 mandates entry of the order); Brown v. Waddell, 50 F.3d 285, 290 (4th Cir. 1995) (Section 3122 does not require the government to establish probable cause to obtain a pen register or trap and trace device); United States v. Newman, 733 F.2d 1395, 1398 (10th Cir. 1984) ("[N]o showing of probable cause -- or even 'sufficient cause,' as defendant suggests -- is necessary to justify authorization of a pen register.")

[45] "Post-cut-through dialed digits," also called "dialed digit extraction features," are any digits that are dialed from the **Subject Telephone Number[s]** after the initial call setup is completed. For example, some post-cut-through dialed digits are telephone numbers, such as when a subject places a calling card, credit card or collect call by first dialing a long-distance carrier access number and then, after the initial call is "cut through," dialing the telephone number of the destination party. That final number sequence is necessary to route the call to the intended party and, therefore, identifies the place or party to which the call is being made. Under these circumstances, the "post-cut-through" digits are the type of information (i.e., "dialing, routing, addressing, or signaling" information) specifically authorized by the statute for capture. Post-cut-through dialed digits also can represent call content, such as when

CHARGES EXTRA $1,500 FOR PEN/TRAP ON DIRECT CONNECT (WALKIE TALKIE) COMMUNICATIONS, INCLUDE PAST FOOTNOTE REQUESTING PEN/TRAP ON "DIRECT CONNECT" ONLY IF AGENTS DECIDE THAT INVESTIGATION WARRANTS REQUEST FOR SUCH DATA] from the **Subject Telephone Number[s]**, to record the date and time of such dialings or transmissions, and to record the length of time the telephone receiver in question is "off the hook" for incoming or outgoing calls, for a period of sixty days from the date the order is filed by the court.

b. The **[name agency} to install, or cause the provider to install, and use [continued use]** trap and trace device[s] on the **Subject Telephone Number[s]** anywhere in the United States to capture and record the incoming electronic or other impulses which identify the originating numbers or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication and to record the date, time, and duration of calls created by such incoming impulses, for a period of sixty days from the date the order is filed by the court.

c. That, pursuant to 18 U.S.C. § 3123(b)(1)©, the requested **[installation and use] [continued use]** of a pen register and trap and trace device permit the use of such a pen register and trap and trace device not only on the **Subject Telephone Number[s]**, but also on any changed telephone number(s) subsequently assigned to an instrument bearing the same ***[insert as appropriate* ESN/IMSI/SIM]** as the **Subject Telephone Number[s]**, or any changed ***[insert as appropriate* ESN/IMSI/SIM]** subsequently assigned to the same telephone number as the **Subject Telephone Number[s]**, or any additional changed telephone number(s) and/or ***[insert as appropriate* ESN/IMSI/SIM]**, whether the changes occur consecutively or simultaneously, listed to the same subscriber and wireless telephone account number as the **Subject Telephone**

---

subjects call automated banking services and enter account numbers, or call voicemail systems and enter passwords, or call pagers and dial call-back telephone numbers (which are considered numeric messages.) To the extent that additional digits that are content are received, the government will not use such information for any investigative purposes.

[46] Including dialing, routing, addressing, or signaling information transmitted over the communication service provider's network by a two-way radio feature (including, but not limited to, Nextel's "Direct Connect/Direct Dispatch," Verizon Wireless' "Push to Talk," or Sprint's "ReadyLink"). The two-way radio feature, like a walkie-talkie, provides communication between similarly equipped cellular phones by pressing a button on the telephone. Like a pen register or trap and trace on a telephone, a pen register or trap and trace for information transmitted by the two-way radio feature will not disclose content of the call.

Number[s];[47] ***[insert as appropriate-Confirm with Tech Agent whether "target filtering" is possible]*** and on any cellular phone that is within close proximity to the government device that may autonomously register with the device,[48] within the 60-day period authorized by this order.

4. Pursuant to 18 U.S.C. § 3123(a)(1) and § 3123(b)(2), I further request that the court direct that upon service of the order upon it, the local, long distance, and wireless carriers listed in the proposed order, any other communications service

---

[47] Section 3123(b)(1)(C) has been amended to require the Court to specify in the order "the attributes of the communications to which the order applies, including the number or other identifier . . . ." 18 U.S.C. § 3123(b)(1)(C). The account number, when combined with the same subscriber name for the **Subject Telephone Number[s]** sufficiently specifies "the attributes of the communications to which the order applies, including the number or other identifier . . ." as required by § 3123(b)(1)(C). Cf. United States v. Duran, 189 F.3d 1071, 1083-1086 (9th Cir. 1999) (holding interception of wire communications on a cellular telephone with a changed telephone number followed by a changed ESN was covered by the order authorizing the interception of wire communications even though the court order authorizing the wiretap only anticipated a changed telephone number but did not anticipate a changed ESN).

[48] This is necessary in order to identify the Subject Telephone to the exclusion of others also operating within a particular cellsite. We respectfully do not concede that a device used to receive radio signals, emitted from a wireless cellular telephone, that merely identify that telephone to the network (i.e., registration data) constitutes a "pen register" or "trap and trace" device. Cf. In the Matter of the Application of the U.S. for an Order Authorizing the Use of a Cellular Telephone Digital Analyzer, 885 F. Supp. 197, 201 (C.D. Cal. 1995) (interpreting prior definition of pen register device and holding that no court order is required to use a digital analyzer to capture cellphone ESN, telephone numbers, and dialed numbers, because the device does not "attach" to a telephone line). We nonetheless submit this request for authorization out of an abundance of caution, on the chance that the device may collect dialed numbers generated by a phone initiating an outgoing call attempt while it is temporarily registered with the device. To the extent such information is incidentally acquired, it is agency policy not to record or retain it or any data associated with non-target telephones. Moreover, the government uses a number of criteria to limit both the collection of data and to minimize any potential temporary disruption of service, most notably by operating the device for limited duration and only when the cellsite information acquired from the provider indicates that the Subject Telephone is operating nearby.

provider providing service to the **Subject Telephone Number[s]**,[49] and any other person or entity providing wire communication service in the United States whose assistance may facilitate execution of the order, furnish forthwith all information, facilities, and technical assistance necessary to accomplish unobtrusively the installation and use of the pen register and trap and trace devices and with minimum interference with the services that are accorded the persons with respect to whom the installation and use is to take place, with compensation to be paid by the investigative agency for reasonable expenses directly incurred in providing such facilities and assistance.

5. I further request that the order direct the local, long distance, and wireless carriers, and any other person or entity providing wire or electronic communication service in the United States whose assistance is used to facilitate execution of the order, to furnish the results of the pen register and trap and trace devices to Special Agents of the **[AGENCY/IES]** as soon as practicable, on a continuing basis, twenty-four (24) hours a day for the duration of the order.

III. SPECIFIC AND ARTICULABLE FACTS ESTABLISHING REASONABLE GROUNDS TO BELIEVE THAT SUBSCRIBER RECORDS AND CELL SITE INFORMATION ARE RELEVANT AND MATERIAL TO AN ONGOING CRIMINAL INVESTIGATION PURSUANT TO 18 U.S.C. § 2703

1. Title 18, United States Code, Section 2703(d) provides that a court may issue an order authorizing disclosure of a record or other information pertaining to a telephone subscriber or customer (not including the contents of communications) when a government agency provides the court with:

> [S]pecific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.

The statute, by its own language, precludes holding the government to a higher standard of proof, such as probable cause. See Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414 § 207(2), reprinted in 1992 U.S. Code Cong. & Admin. News 4292. The House Report reflected that "[t]*his section imposes an* intermediate standard to protect on-line transactional records.

---

[49] The reference to "another communication service provider" is necessary so that the court order is still effective in the event that the **Subject Telephone Number[s] [is] [are]** transferred to another carrier pursuant to "Local Number Portability" ("LNP"). LNP allows a telephone user to change his/her telephone company but still keep the same telephone number. However, to transfer (i.e. "port") a telephone number pursuant to LNP, the subscriber information must remain the same. Thus, this reference applies if the **Subject Telephone Number[s] [is] [are]** transferred (i.e. "ported") to another telephone carrier, but the telephone number and subscriber information remain the same.

It is a standard higher than a subpoena, but not a probable cause warrant." See H.R. Rep. No. 103-827, at 31-32 (1994), reprinted in 1994 U.S.C.A.A.N. 3489, 3511-12.[50]

2. For the purposes of obtaining a court order for disclosure as described in 18 U.S.C. § 2703(c)(1), and in order to satisfy the requirements of 18 U.S.C. § 2703(d), government counsel, based on discussions with SA **[AGENT'S NAME]**, hereby sets forth the following specific and articulable facts showing that there are reasonable grounds to believe that the records or other information identifying subscribers (but not including the contents of communications) for telephone numbers identified through the pen register and trap and trace device on **the Subject Telephone Number[s]**, cell site information regarding the **Subject Telephone Number[s]**, subscriber information associated with any service changes regarding the **Subject Telephone Number[s]**, [and the records or other information pertaining to subscribers (but not including the contents of communications) for the **Subject Telephone Number[s]]** will be relevant and material to an ongoing criminal [fugitive] investigation:

a. **[INSERT SUMMARY OF FACTS RELATING TO INVESTIGATION AND RELEVANCE OF SUBJECT TELEPHONE NUMBER[S] TO INVESTIGATION. PLEASE BE AWARE THAT THIS SECTION IS SEPARATE FROM THE CERTIFICATION UNDER SECTION 3122 BECAUSE IT IS MADE PURSUANT TO SECTION 2703(d), WHICH REQUIRES A PRESENTATION OF PROOF, NOT MERELY A CERTIFICATION. IN ORDER TO OBTAIN A SECTION 2703 ORDER, WE MUST PRESENT "SPECIFIC AND ARTICULABLE FACTS ESTABLISHING REASONABLE GROUNDS TO BELIEVE THAT SUBSCRIBER INFORMATION AND CELL SITE INFORMATION ARE RELEVANT AND MATERIAL TO AN ONGOING CRIMINAL INVESTIGATION." (THIS IS A LOWER STANDARD THAN PROBABLE CAUSE.) AS A RESULT, YOU NEED TO MAKE SURE YOU SET FORTH SPECIFIC FACTS RE: YOUR INVESTIGATION, WHY AGENT THINKS TARGET(S) IS/ARE USING THE SUBJECT TELEPHONE(S), AND WHY GETTING SUBSCRIBER AND CELL SITE INFORMATION IS RELEVANT TO YOUR INVESTIGATION. YOU CAN ALSO INCLUDE ANY RELEVANT EXPERT OPINIONS OF YOUR AGENTS. TRY TO LIMIT THIS SECTION TO 4-5 PARAGRAPHS, ALTHOUGH MORE MAY BE NECESSARY DEPENDING ON THE CASE. IF QUOTING WIRETAPPED CALLS OVER THE SUBJECT TELEPHONE, USE NO MORE THAN TWO CALLS PER TELEPHONE AND**

---

[50] Persons calling to and from the **Subject Telephone Number[s]** do not have a Fourth Amendment privacy interest regarding their subscriber information. United States v. Fregoso, 60 F.3d 1314, 1321 (8th Cir. 1995) (rejecting defendant's challenge to court order permitting phone company to supply subscriber information "for the telephone numbers obtained from the pen register and the caller identification service," holding, "We agree with the magistrate judge's assessment that because this information is listed in phone books and city directories, and at a bare minimum revealed to the phone company to obtain telephone service, there can be no expectation that this information will remain private."). See Smith v. Maryland, 442 U.S. 735, 742-44 (1979) ("a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.")

INCLUDE AGENT'S INTERPRETATION OF ANY CODED LANGUAGE. IF WIRETAPPED CALL IS LENGTHY, SUMMARIZE.]

IMPORTANT: THE MAGISTRATE JUDGES NOW REQUIRE THAT IF THIS IS AN EXTENSION OF A PEN/TRAP ON SUBJECT TELEPHONE[S], YOU MUST INCLUDE A PARAGRAPH CONTAINING THE DATE, MISC. NO. AND SIGNING JUDGE OF ANY PRIOR PEN REGISTER ORDERS ON EACH SUBJECT TELEPHONE[S] IN YOUR CASE AND A SUMMARY OF THE RESULTS OF THE PRIOR PENS DURING THE MOST RECENT 60-DAY PERIOD. IF SUMMARY OF PAST PEN[S] DOES NOT INDICATE CRIMINAL ACTIVITY, JUDGE MAY NOT GRANT REQUESTED EXTENSION.

b. [INSERT EXPLANATION AS TO WHY RECORDS OR OTHER INFORMATION IDENTIFYING SUBSCRIBERS FOR TELEPHONE NUMBERS OBTAINED THROUGH THE PEN REGISTER AND TRAP AND TRACE DEVICES ON THE SUBJECT TELEPHONE NUMBER[S] ARE RELEVANT AND MATERIAL TO YOUR INVESTIGATION. THE FOLLOWING IS A SAMPLE FOR NARCOTICS CASES, WHICH YOU MAY ADAPT TO YOUR CASE: Based upon SA [AGENT'S NAME's] experience, information identifying the subscribers for numbers obtained from numbers captured by the pen register and the trap and trace devices, and subscriber information associated with any service changes, has yielded information that is relevant and material to narcotics trafficking investigations. Such information includes leads relating to: (1) the names of suspected suppliers, customers and other individuals who assist in the distribution of narcotics; (2) the location of "stash" houses where narcotics are stored; (3) the identity of transportation sources used by the drug traffickers; (4) the locations of money transfer businesses used by members of the operation to launder proceeds of drug trafficking activities or through which money is exchanged with coconspirators ; (5) the geographic breadth of the suspected drug trafficking cell; and (6) the identities of potential organizers, leaders, managers, or supervisors of the suspected trafficking cell by examining the calling patterns revealed by the toll data. SA [AGENT'S NAME] has advised me that, based upon [his] [her] training and experience, one way to identify coconspirators is to evaluate the pattern of calls and to obtain information identifying subscribers for calls made to and from the Subject Telephone Number[s] which could be potential coconspirators and then to conduct an investigation concerning those individuals. Based upon the subscriber information, SA [AGENT'S NAME] would also direct other investigators to conduct surveillance at the addresses and determine if criminal activity was occurring there, which in turn could yield potential names of coconspirators and potential narcotics storage locations used by the organization.

Obtaining the subscriber name, address, date of birth, social security number, driver's license information, contact names and numbers, employment information, and method of payment is critical to accurately identifying such subscribers because, among other things: (1) if the subscriber name is a common one and/or the subscriber address is not current, it can be difficult to accurately identify the subscriber without a date of birth, driver's license or social security number, especially in an area with a population as the Central District of California; (2) if the subscriber name and address is fictitious, which frequently is the case when criminals purchase telephones, all or part of the remaining identification information may be truthful and help identify the subscriber or lead to identifying other

coconspirators; (3) by accurately identifying subscribers using the above-requested information, agents can eliminate innocent individuals as targets.

[IF FUGITIVE INVESTIGATION, INSERT THE FOLLOWING: In [AGENT'S] experience, information identifying subscribers for numbers obtained from numbers captured by the pen register and the trap and trace devices, and subscriber information associated with any service changes, has yielded information that is relevant and material to a fugitive investigation. Such information includes leads relating to the names of family members, associates, friends and other individuals who may assist in the apprehension of the fugitive or may aid in the harboring of the fugitive. [AGENT] has advised me that one way to identify associates may be to obtain information identifying subscribers for calls made to and from the Subject Telephone Number and then conduct an investigation concerning those individuals. Based upon the identifying information, [AGENT] would then direct other investigators to monitor those addresses and determine if the fugitive is present or if the associates or family members may lead investigators to him.]

c. **[INSERT FOLLOWING EXPLANATION AS TO WHY CELL SITE INFORMATION IS NEEDED FOR THE SUBJECT TELEPHONE NUMBER[S]:** The investigating agents have further advised me that the general geographic location of the **Subject Telephone Number[s]** derived from cell site information used by the **Subject Telephone Number[s]** can be used to corroborate the observations of surveillance agents. More specifically, surveillance agents can compare observations of the user of the **Subject Telephone Number[s]** with cell site information in order to verify the identification and proximate location of the user of the **Subject Telephone Number[s]**.

[INSERT IF REQUESTING TOLL/CALL DETAIL RECORDS: d. INSERT EXPLANATION AS TO WHY YOU NEED RECORDS OR OTHER INFORMATION PERTAINING TO SUBSCRIBERS OF THE SUBJECT TELEPHONE NUMBER[S]. FOR FUGITIVE CASES: Historical records (i.e. toll information and/or call detail records) for the Subject Telephone Number[s] are important in fugitive investigations to establish a past pattern of activity for the fugitive (i.e. where he/she has been, who he/she has been calling) because it helps to determine where the fugitive is at now. The government is requesting historical records for a [NUMBER OF DAYS, I.E. 30 OR 60]-day period because [EXPLAIN NEED FOR PARTICULAR PERIOD OF TIME].

3. Accordingly, based upon the above proffer, and pursuant to 18 U.S.C. §§ 2703(c)(1)(B) and 2703(d), because there are reasonable grounds to believe that such information is relevant and material to the ongoing investigation, I further request that the court issue an order requiring the providers listed in the proposed order, lodged concurrently herewith, and any other person or entity providing wire or electronic communications service in the United States whose assistance may facilitate execution of the order, to disclose, or provide upon oral or written request by Special Agents of the **[AGENCY/IES]** the information set forth above in paragraph A2.

D. REQUEST THAT ORDER PRECLUDE NOTICE AND THAT APPLICATION AND ORDER BE FILED UNDER SEAL

1. Based upon the information provided in this application, I believe disclosure of the requested court order may result in flight from potential prosecution or the destruction of or tampering with evidence, or may otherwise seriously jeopardize the investigation. Moreover, the exact nature of the government "pen register" device and its configuration is classified as a law enforcement sensitive investigative technique, the disclosure of which would likely jeopardize other on-going investigations, and/or future use of the technique. Therefore, pursuant to 18 U.S.C. §§ 2705(b) and 3123(d), I request that this application and order be sealed and that the court direct the local, long distance, and wireless carriers listed in the proposed order, any internet service provider or other electronic communications provider providing voice-over IP telephony,[51] and any other local, long distance, or wireless carrier servicing the **Subject Telephone Number[s]** who is obligated by the order to provide assistance to the Applicant, not to disclose in any manner, directly or indirectly, by any action or inaction, to the listed subscriber(s) for the **Subject Telephone Number[s]**, the occupant of said premises, the subscribers of the incoming calls to or outgoing calls from the **Subject Telephone Number[s]**, or to any other person, the existence of this order, in full or redacted form, of the pen register or trap and trace devices, or of this investigation, unless otherwise ordered by this court.

2. I further request that the identity of any targets of the investigation may be redacted from any copy of the order served on any service provider or other person, and that this order and application be SEALED until otherwise ordered by the court.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief, and that this declaration was executed on [**DATE**] at [**CITY**], California.

[**WARNING!! ONE LAST THING: BEFORE FILING, SEARCH FOR ALL BRACKETS IN APPLICATION AND ORDER TO MAKE SURE THAT ALL BRACKETS HAVE BEEN DELETED, ALL BRACKETED PHRASES HAVE BEEN FILLED IN OR DELETED, AND THAT YOU HAVE REMOVED ALL BOLD EXCEPT FOR "SUBJECT TELEPHONE NUMBER[S]"****

_____

[**YOUR NAME**]

Assistant United States Attorney

---

[51] Voice-over Internet Protocol telephony, also called Voice-over IP or VoIP, is essentially a type of hardware and software that allows people to use the internet as a transmission medium for telephone calls. In general, this means sending voice information in the form of digital packets of information rather than sending it through the traditional public switch telephone network. Like a pen register or trap and trace on traditional telephone service, a pen register or trap and trace for VoIP service will not disclose the contents of the call.

[**INSERT SECTION**] Section

Combined 3123/2703 Order

[NAME]
United States Attorney
[NAME]
Special Assistant United States Attorney
Chief, Criminal Division
[YOUR NAME]
Assistant United States Attorney
[_____] Section
State Bar No. [_____]
[ADDRESS]
[CITY, STATE ZIP]
Telephone: (XXX)-[____]
Facsimile: (XXX) -[____]

Attorneys for Applicant
United States of America

UNITED STATES DISTRICT COURT

FOR THE [XXXX] DISTRICT OF [STATE]

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER:(1) AUTHORIZING THE INSTALLATION AND USE OF A PEN REGISTER AND A TRAP AND TRACE DEVICE; AND (2) AUTHORIZING RELEASE OF SUBSCRIBER INFORMATION, AND CELL SITE INFORMATION	No. _____ **[NOTE: INSERT SAME AS APPLIC]** [PROPOSED] ORDER (UNDER SEAL)

This matter having come before the court pursuant to an application under Title 18, United States Code, Sections 2703© and

(d), 3122, and 3123, by Assistant United States Attorney **[YOUR NAME]**, an attorney for the Government as defined by Fed. R. Crim. P. 1(b)(1), requesting an order authorizing the **[installation and use] [continued use]** of a pen register and trap and trace device, on the following telephone number**[s]**:

(a) **[REPEAT <u>EXACT</u> SAME INFORMATION FROM APPLICATION REGARDING SUBJECT TELEPHONE NUMBER[S], BUT WITHOUT FOOTNOTES]** and

UPON REVIEW OF THE APPLICATION, THE COURT HEREBY FINDS THAT:

Pursuant to 18 U.S.C. § 3123, Applicant has certified that the information likely to be obtained by such use is relevant to an ongoing criminal investigation being conducted by the **[AGENCY/IES]** in connection with possible violations of **[DESCRIBE <u>EXACTLY</u> AS IN APPLICATION]**.

THEREFORE, IT IS HEREBY ORDERED, pursuant to 18 U.S.C. § 3123, that Special Agents of the **[AGENCY/IES]** may **[install, or cause to be installed, and use] [continue to use]** a pen register anywhere in the United States to record or decode dialing, routing, addressing , or signaling information (including "post-cut-through dialed digits"[1]) **[**[2]**]** **[<u>NOTE</u>: INCLUDE FOOTNOTE 2 ONLY IF**

---

[1] "Post-cut-through dialed digits," also called "dialed digit extraction features," are any digits that are dialed from the **Subject Telephone Number[s]** after the initial call set-up is completed, subject to the limitations of 18 U.S.C. § 3121(c). To the extent additional digits that are received are content, the government shall not use such information for any investigative purposes or attempt to decode such information.

[2] Including dialing, routing, addressing, or signaling information transmitted over the communication service provider's network by a two-way radio feature (including, but not limited to, Nextel's "Direct Connect/Direct Dispatch," Verizon Wireless' "Push

REQUESTED IN APPLICATION] transmitted from the **Subject Telephone Number**, to record the date and time of such dialings or transmissions, and to record the length of time the telephone receiver in question is "off the hook" for incoming or outgoing calls, for a period of sixty days from the date this order is filed by the court;[3]

IT IS FURTHER ORDERED, pursuant to 18 U.S.C. § 3123, that Special Agents of the **[AGENCY/IES]** may install, or cause to be installed, and use a trap and trace device on the **Subject Telephone Number[s]** anywhere in the United States to capture and record the incoming electronic or other impulses which identify the originating numbers or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication, and to record the date, time, and duration of calls created by such incoming impulses, for a period of sixty days from the date this order is filed by the court;

Pursuant to 18 U.S.C. §§ 2703(c)(1)(B) and 2703(d), Applicant has set forth specific and articulable facts showing that there are reasonable grounds to believe that records or other information identifying subscribers or customers (not including the contents of communications) for telephone numbers identified through the pen register and trap and trace devices on the **Subject Telephone Number[s]**, changes in service regarding the **Subject Telephone Number[s]**, cell site information regarding the **Subject**

---

to Talk", or Sprint's "ReadyLink").

[3] As used herein, "the date this order is filed by the court" is the date indicated by the clerk's file stamp on the first page of this order.

Telephone Number[s], and records or other information pertaining to subscribers or customers (but not including the contents of communications) for the **Subject Telephone Number[s]** will be relevant and material to an ongoing criminal investigation.

THEREFORE, IT IS FURTHER ORDERED, pursuant to 18 U.S.C. §§ 2703(c)(1)(B), 2703(c)(2) and 2703(d), that SBC Communications, Inc. or any subsidiary thereof, Ameritech, Southern New England Telephone Company, Verizon California, Inc., XO Communications, Comcast Cable Communications Inc./AT&T Corporation, Verizon New York, Inc., MPower Communications, Verizon New Jersey Inc., Bell South Telephone Company, Allegiance Telecom, Cox Communications and Qwest Communications (hereinafter the "local carriers"); AT&T, U.S. Sprint, and MCI (hereinafter the "long distance carriers"); Cellco Partnership, dba Verizon Wireless, AT&T Wireless Services, U.S. Cellular, MetroPCS, Cingular Wireless, Nextel Partners, Cricket Communications, Sprint Spectrum L.P., T-Mobile USA, Inc., Virgin Mobile USA, Nextel Communications and Western Wireless Corp. (hereinafter "the wireless carriers");

any internet service provider or other electronic communications provider providing voice-over IP telephony, <u>and any other</u> local, long distance, or wireless carrier servicing the **Subject Telephone Number[s]**, and any other person or entity providing wire communication service in the United States whose assistance may facilitate execution of the order, shall disclose or provide the following upon oral or written request by Special Agents of the **[AGENCY/IES]**:

1. Records or other information identifying subscribers or customers (but not including the contents of communications or toll records), namely, subscriber name, address, date of birth,

social security number, driver's license (state and number), contact names and numbers, employment information, method of payment, length of service, and type of service utilized, for all published, non-published, listed, or unlisted numbers, dialed or otherwise transmitted to and from the **Subject Telephone Number[s]**;

2. All changes (including additions, deletions, and transfers) in service regarding the **Subject Telephone Number[s]** to include telephone numbers and subscriber information (published, non-published, listed, or unlisted) associated with these service changes; [and]

3. For the **Subject Telephone Number[s]**,records or other information pertaining to subscriber(s) or customer(s), including historical cellsite information and call detail records [including direct connect records[4]] for the following dates: _____ to the present **[THE LAST TEN DAYS IS RECOMMENDED]** (but not including the contents of communications).

d. For the **Subject Telephone Number[s]**, all cellsite information[5] provided to the government on a continuous basis contemporaneous with call origination (for outbound calling) and call termination (for incoming calls), or at such other time upon

---

[4] **ASK TECH AGENT: DEFINE DIRECT CONNECT. OR BETTER YET, IS THERE A GENERIC TERM, SUCH AS WALKIE TALKIE FEATURE OR TWO WAY RADIO FEATURE??**

[5] "Cellsite information" refers categorically to any and all data associated with registration of the Subject Telephone with cellsites/network, as well as other data used by the network to establish a connection with the telephone handset and to maintain connectivity to the network. This includes the physical location and/or address of the cellular tower, cellsite sector, control channel number, neighbor cell lists, and any identification numbers, processing data, and parameters not pertaining to the contents of a call.

the oral or written request of the government, including if reasonably available, during the progress of a call.

IT IS FURTHER ORDERED that this authorization for the **[installation and use] [continued use]** of a pen register and trap and trace device applies not only to the **Subject Telephone Number[s]** listed above, but also to any changed telephone number(s) subsequently assigned to an instrument bearing the same **[*insert as appropriate* ESN/IMSI/SIM]** as the **Subject Telephone Number[s]** or any changed **[*insert as appropriate* ESN/IMSI/SIM]** subsequently assigned to the same telephone number as the **Subject Telephone Number[s]**, or any additional changed telephone number(s) and/or **[*insert as appropriate* ESN/IMSI/SIM]**, whether the changes occur simultaneously or consecutively, listed to the same subscriber and wireless telephone account as the **Subject Telephone Number[s]**, ***[insert only if requested in application-Confirm with Tech Agent]*** and on any cellular phone that is within close proximity to the government device that may autonomously register with the device,[6] within the 60-day period authorized by this order;

IT IS FURTHER ORDERED, pursuant to 18 U.S.C. §§ 3123(a)(1) and § 3123 (b)(2), that upon service of this order upon it, the local, long distance, and wireless carriers listed herein, any other communications service provider providing service to the **Subject Telephone Number[s]**, and any other person or entity providing wire communication service in the United States whose assistance may facilitate execution of this order, shall furnish

---

[6] Once the **Subject Telephone** is identified and located any data incidentally collected from non-target telephones shall not be recorded or retained.

Special Agents of the [**AGENCY/IES**] forthwith all information, facilities, and technical assistance necessary to accomplish unobtrusively the installation and use of the pen register and trap and trace devices and with minimum interference with the services that are accorded the persons with respect to whom the installation and use is to take place;

IT IS FURTHER ORDERED that the local, long distance, and wireless carriers, and any other person or entity providing wire or electronic communication service in the United States whose assistance is used to facilitate execution of the order, furnish the results of the pen register and trap and trace devices to Special Agents of the [**AGENCY/IES**] as soon as practicable, on a continuing basis, twenty four (24) hours a day for the duration of the order.

IT IS FURTHER ORDERED that the local, long distance, and wireless carriers be compensated by the investigative agency for reasonable expenses directly incurred in providing technical assistance; and,

Good cause having been shown, IT IS FURTHER ORDERED, pursuant to 18 U.S.C. §§ 2705(b) and 3123(d), that this order and the application be sealed until otherwise ordered by the court,

and that the local, long distance, and wireless carriers listed herein, any internet service provider or other electronic communications provider providing voice-over IP telephony, <u>and any other</u> local, long distance, or wireless carrier servicing the **Subject Telephone Number[s]** who is obligated by the order to provide assistance to the Applicant, shall not disclose in any manner, directly or indirectly, by any action or inaction, to the listed subscriber(s) for the **Subject Telephone Number[s]**, the

occupant of said premises, the subscribers of the incoming calls to or outgoing calls from the **Subject Telephone Number[s]**, or to any other person, the existence of this order, in full or redacted form, of the pen register or trap and trace devices, or of this investigation, unless otherwise ordered by this court.

IT IS FURTHER ORDERED that the identity of any targets of the investigation may be redacted from any copy of the order served on any service provider or other person, and that this order and application be SEALED until otherwise ordered by the court.

******WARNING!! ONE LAST THING: BEFORE FILING, SEARCH FOR ALL BRACKETS ("]" IN APPLICATION AND ORDER TO MAKE SURE THAT ALL BRACKETS HAVE BEEN DELETED, ALL BRACKETED PHRASES HAVE BEEN FILLED IN OR DELETED AND THAT YOU HAVE REMOVED ALL BOLD EXCEPT FOR "SUBJECT TELEPHONE NUMBER[S]"******

DATED: _____

_____

[INSERT DUTY MAG JUDGE'S NAME]
UNITED STATES MAGISTRATE JUDGE

Presented by:

_____

[YOUR NAME]
Assistant United States Attorney
[**INSERT SECTION**] Section

Application for Video Surveillance

UNITED STATES DISTRICT COURT
_____ DISTRICT OF _____

_____
)
IN THE MATTER OF THE APPLICATION)
OF THE UNITED STATES FOR AN ORDER)
AUTHORIZING THE INTERCEPTION OF)
VISUAL, NON-VERBAL CONDUCT AND)
ACTIVITIES BY MEANS OF CLOSED)
CIRCUIT TELEVISION OCCURRING)
WITHIN THE PREMISES KNOWN AS)
_____)
_____)

APPLICATION FOR AN ORDER AUTHORIZING THE
INTERCEPTION OF VISUAL, NON-VERBAL CONDUCT AND
ACTIVITIES BY MEANS OF CLOSED CIRCUIT TELEVISION

A. Pursuant to Rule 41(b) of the Federal Rules of Criminal Procedure, the United States of America by and through _____, United States Attorney for the _____ District of _____, and _____, an Assistant United States Attorney for said District, hereby makes application to this Court for an order authorizing the interception and recording of visual, non-verbal conduct and activities by means of closed circuit television occurring within the following premises: (set forth a particularized description of the premises to be surveilled.) The factual basis for the granting of this application is set forth in the attached affidavit of _____, which is incorporated by reference herein.

B. Also attached to this application is a letter from the Director (or the Senior Associate Director or Associate Director), Office of Enforcement Operations, Criminal Division, United States Department of Justice, authorizing the making of this application for visual surveillance by means of closed circuit television.

C. The attached affidavit of _____ reflects that there is probable cause to believe:

1. The premises known as _____, located at _____, are being and will continue to be

used by (name the interceptees), to commit offenses involving (list the violations).

2. The visual, non-verbal conduct and activities of the above-named individual(s) will be obtained through interception by means of closed circuit television at these premises and that such conduct and activities will provide:

a. information indicating the precise nature, scope, extent and methods of operation of the participants in the illegal activities referred to above,

b. information reflecting the identities and roles of accomplices, aiders and abettors, co-conspirators, and participants in the illegal activities referred to above, and

c. admissible evidence of commission of the offenses described above.

3. Installation of electronic visual surveillance equipment may require surreptitious entry into the premises (by breaking and entering, if necessary).

4. Normal investigative procedures have been tried and failed or reasonably appear unlikely to succeed, if tried, or appear to be too dangerous to employ.

5. On the basis of the attached affidavit of _____ and allegations contained in this application,

IT IS HEREBY REQUESTED that this Court authorize Special Agents of the (name the investigative agency/agencies) to intercept and record by means of closed circuit television visual, non-verbal conduct and activities of (name the interceptees) and others as yet unknown within the premises known as _____, located at _____, concerning offenses, involving (list the violations).

IT IS REQUESTED FURTHER that such interception not automatically terminate when the type of visual, non-verbal conduct described above has first been obtained but continue until conduct is intercepted that reveals: (1) the manner in which the above-named described offenses are being committed; (2) the precise nature, scope, and extent of the above-described offenses, and, (3) the identity and roles of accomplices, aiders and abettors, co-conspirators, and participants, or for a period of thirty (30) days from the date of this order, whichever is earlier.

IT IS REQUESTED FURTHER that Special Agents of the (name the investigative agency/agencies) be authorized to enter the above-described premises surreptitiously, covertly, and by breaking and entering, if necessary, in order to install, maintain and remove electronic visual surveillance equipment used by the (name the investigative agency/agencies) to intercept and record visual, non-verbal conduct occurring within the foregoing premises.

IT IS REQUESTED FURTHER THAT this order require that it be executed as soon as practicable and that interception be conducted in such a manner as to minimize interception of visual, non-verbal conduct which is not criminal in nature, and that the order terminate upon attainment of the authorized objectives or at the end of thirty (30) days from the date of the order, whichever is earlier.

IT IS REQUESTED FURTHER that surveilling agents be authorized to spot monitor the premises to ascertain whether any of the aforementioned persons are present inside the premises.

When such persons are found to be present, the agents will continue the interception as to conduct that involves the designated offenses.

When it is determined that none of the named interceptees nor any person subsequently identified as an accomplice who uses the premises to commit or converse about the designated offense(s) is inside the premises, interception of visual, non-verbal conduct will be discontinued.

IT IS REQUESTED FURTHER that, in accordance with 18 U.S.C. 3103a(b), this Court's order delay notification of the execution of the order for a period not to exceed ninety days (or some lesser period) because there is reasonable cause to believe that providing immediate notification would seriously jeopardize the investigation. Such period of delay may thereafter be extended by the court for good cause shown.

Dated: _____, 20___

Respectfully submitted,

_____

Assistant United States Attorney

Order for Video Surveillance

UNITED STATES DISTRICT COURT
_____ DISTRICT OF _____

_____
)
IN THE MATTER OF THE APPLICATION)
OF THE UNITED STATES FOR AN)
ORDER AUTHORIZING THE INTERCEPTION)
OF VISUAL, NON-VERBAL CONDUCT)
AND ACTIVITIES BY MEANS OF CLOSED)
CIRCUIT TELEVISION OCCURRING)
WITHIN THE PREMISES KNOWN AS)
_____)
_____)

ORDER
AUTHORIZING THE INTERCEPTION OF VISUAL,
NON-VERBAL CONDUCT AND ACTIVITIES

Application under oath having been made before me by _____, Assistant United States Attorney for the _____ District, for an order authorizing the interception and recording of visual, non-verbal conduct and activities pursuant to Rule 41(b) of the Federal Rules of Criminal Procedure and full consideration having been given to the matters set forth therein, the Court finds:

A. There is probable cause to believe that _____ and others as yet unknown have committed and are committing offenses involving (list the offenses).

B. There is probable cause to believe that particular visual, non-verbal conduct and activities concerning these offenses will be obtained through the interception for which authorization is herewith applied. In particular, visual, non-verbal conduct and activities will concern the (characterize the offenses).

C. Normal investigative procedures have been tried and failed, reasonably appear unlikely to succeed if tried or continued, or are too dangerous.

D. There is probable cause to believe that the premises (located at)(known as) _____ have been and are

being used by _____ and others as yet unknown, in connection with the commission of the above-stated offenses.

WHEREFORE, IT IS HEREBY ORDERED that the (name of the investigative agency/agencies) is authorized, to intercept and record the visual, non-verbal conduct and activities of (name interceptees) and others as yet unknown, concerning the above-described offenses at the premises located at _____). Such interception shall not terminate automatically when the type of conduct/ activity described above in paragraph (B) has first been observed but shall continue until the conduct or activity is intercepted that reveals the manner in which (name the interceptees), and others as yet unknown participate in the specified offenses and reveals the identities of (his)(their) coconspirators, their methods of operation, and the nature of the conspiracy, or for a period of (state the time period not to exceed 30 days), whichever is earlier.

IT IS ORDERED FURTHER that special agents of the (name of the investigative agency/agencies) are authorized to enter the foregoing premises surreptitiously for the purpose of installing, maintaining, and removing any electronic monitoring devices utilized pursuant to the authority granted by this order.

PROVIDING THAT, this authorization to intercept visual, non-verbal conduct and activities shall be executed as soon as practicable after the signing of this order and shall be conducted in such a way as to minimize the interception of conduct and activities not otherwise subject to interception, and must terminate upon attainment of the authorized objective or, in any event, at the end of (not to exceed 30) days.

IT IS ORDERED FURTHER that, in accordance with 18 U.S.C. 3103a(b), notification of the execution of this order be delayed for a period not to exceed ninety days (or some lesser period) because there is reasonable cause to believe that providing immediate notification would seriously jeopardize the investigation. Such period of delay may thereafter be extended by the court for good cause shown.

_____

JUDGE

Date: _____

Application for Disclosure

UNITED STATES DISTRICT COURT
_____ DISTRICT OF _____

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER AUTHORIZING THE DISCLOSURE OF INTERCEPTED WIRE, ORAL AND/OR ELECTRONIC COMMUNICATIONS.	))))))

APPLICATION

_____, an Attorney for the United States Department of Justice (or an Assistant United States Attorney) states:

A. I am an "investigative or law enforcement officer of the United States" within the meaning of 18 U.S.C. § 2510(7), that is, an attorney authorized by law to prosecute violations of federal law.

B. I am also an "attorney for the government" as defined in Rule 1(b)(1) of the Federal Rules of Criminal Procedure, and, therefore, pursuant to 18 U.S.C. § 2516(1) and (3) and 18 U.S.C. § 2518(8)(b), am authorized to make application to a federal judge of competent jurisdiction for authorization to disclose the application, order and contents of intercepted wire, oral and/or electronic communications upon a showing of good cause pursuant to 18 U.S.C. § 2518(8)(b).

C. This application seeks authorization to disclose intercepted wire, oral and/or electronic communications of (name of the interceptee(s)) relating to felony violations of federal law, that is violations of (characterize the offenses) which were intercepted pursuant to a court order issued by Judge _____ of this court on the _____ day of _____, 20__. Extensions of said order were issued on (use, if appropriate). The order was terminated on the _____ day of _____, 20__. The tapes herein were sealed pursuant to order of the court on the _____ day of _____, 20__.

(If appropriate, state: "The tapes were unsealed on the ___ day of _____, 20__, by order of the court in

connection with the litigation of (name the case) and resealed on the _____ day of _____, 20__.

1) The wire communications were intercepted over telephone _____, located at _____, subscribed to by _____, and/or

2) Electronic communications were intercepted over (describe the facility) listed in the name of _____ and located at _____, and/or

3) Oral communications were intercepted at (identify the location) owned or leased by _____.

D. Disclosure of the intercepted wire, oral and/or electronic communications is sought in connection with

(Here describe the reason(s) for disclosure and the proceeding in which the intercepted communications will be disclosed.)

Attached is the affidavit of (indicate the affiant's name and agency) setting forth a complete statement of facts which, in the opinion of the applicant, provide good and sufficient cause for the disclosure of the intercepted communications pursuant to 18 U.S.C. § 2518(8)(b).

E. Based on my knowledge, information and belief, I know of no previous application for the relief sought herein having been made to any judge or court except as is set forth herein.

(If a prior application was made for disclosure, it should be set forth here and reflect the action of court)

F. On the basis of the facts set forth in the affidavit of (specify the agent) accompanying this application and attached hereto, the applicant requests this court to issue an order, pursuant to the authority conferred on it by 18 U.S.C. § 2518(8)(b) authorizing the disclosure of the wire, oral and/or electronic communications described herein in connection with the proceeding heretofore described.

G. Use only if appropriate, the following: "The applicant requests further that the order incorporate the following

limitations on disclosure in order to protect the rights of confidential sources or innocent third parties."

(Describe here the limitations that should be placed on the disclosure, if any, and give the reasons.)

H. I request further that the court order indicate that this order does not affect any lawful disclosures that could otherwise be made pursuant to the provisions of 18 U.S.C. § 2517.

I declare under penalty of perjury pursuant to 28 U.S.C. § 1746 that the foregoing is true and correct to the best of my knowledge, information and belief.

Executed on _____, 20__.

_____

Applicant

Order for Disclosure of Interceptions

UNITED STATES DISTRICT COURT
_____ DISTRICT OF _____

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES FOR AN ORDER AUTHORIZING THE DISCLOSURE OF INTERCEPTED WIRE, ORAL AND/OR ELECTRONIC COMMUNICATIONS	)

ORDER AUTHORIZING THE DISCLOSURE OF
INTERCEPTED WIRE, ORAL AND/OR ELECTRONIC
COMMUNICATIONS

Application under penalty of perjury having been made before me by _____, an "investigative or law enforcement officer" as defined in 18 U.S.C. § 2510(7) and an "attorney for the government" as defined in Rule 1(b)(1) of the Federal Rules of Criminal Procedure, for an order authorizing the disclosure of applications, orders and intercepted communications, intercepted pursuant to 18 U.S.C. § 2510 et seq. and full consideration having been given to the matters set forth herein, the court finds:

A. There is good and sufficient cause to disclose wire, oral and/or electronic communications of (name the interceptee(s)) intercepted during the period (set forth period in question) over facilities (here describe wire, oral or electronic facilities), pursuant to an order of this court on the _____ day of _____ 20_____, for use in connection with

(Here, describe the proceedings they are to be disclosed in connection with.)

B. (Use only if appropriate) To protect the identity of confidential sources and innocent third parties the following restrictions are placed on this disclosure unless and until further ordered by the court:

Disclosure is not be made with regard to

(here place restrictions, if any. Clarify exact information sought to be restricted.)

C. Nothing in this order shall affect the disclosure of information relating to intercepted communications, the disclosure of which would otherwise be lawful under 18 U.S.C. § 2517.

Wherefore, it is hereby ordered that (subject to the restrictions set forth herein) (name the investigative agency/agencies) is authorized, pursuant to an application made by (applicant) pursuant to authority set forth in 18 U.S.C. §§ 2516(1) and (3) and 2518(8)(b) to disclose intercepted wire, oral and/or electronic communications in connection with the proceedings heretofore described.

_____
UNITED STATES DISTRICT COURT JUDGE

_____
(Date)

Section 2517(5) Application for Testimonial Use
of Interceptions Relating to "Other Offenses"

UNITED STATES DISTRICT COURT
_____DISTRICT OF_____

IN THE MATTER OF THE APPLICATION	)	
OF THE UNITED STATES FOR AN ORDER	)	No. _____
AUTHORIZING THE INTERCEPTION OF	)	
(WIRE/ORAL/ELECTRONIC	)	
COMMUNICATIONS)	)	

APPLICATION FOR AN ORDER AUTHORIZING THE
DISCLOSURE AND USE OF INTERCEPTED COMMUNICATIONS
PURSUANT TO SECTION 2517(5), TITLE 18, UNITED STATES CODE

_____, [an Assistant United States Attorney for the _____ District of _____,][7] being duly sworn, states:

This application is submitted in support of a request for an Order pursuant to the provisions of Title 18, United States Code, Section 2517(5), authorizing the disclosure and use of communications intercepted pursuant to the provisions of Chapter 119, Title 18, United States Code as evidence, while giving testimony under oath, as authorized in Section 2517(3), Title 18 United States Code, in any proceeding held under the authority of the United States relating to a prosecution for violations of Section [ ], Title 18, United States Code, relating to (describe the offense(s)) and in support thereof states as follows:

1) I am an "investigative or law enforcement officer of the United States" within the meaning of Section 2510(7), Title 18, United States Code -- that is, (s)he is an attorney authorized by law to prosecute or participate in the prosecution of offenses enumerated in Section 2516, Title 18, United States Code:

[7] In the alternative, state "an attorney of the United States Department of Justice," if the applicant is a Criminal Division attorney.

2) On _____, United States District Judge _____, _____ District of _____, entered an order in (specify the case number), authorizing Special Agents of the (identify the investigative agency/agencies) to intercept for a _____ day period (wire/oral/electronic) communications of _____, _____, _____, and others as yet unknown (over the telephone(s) (or facsimile machine/pager) bearing the number(s) _____, _____, and _____, listed to _____, at _____) and/or (occurring at the premises known as _____, located at _____) for the purpose of obtaining evidence concerning the commission of offenses enumerated in Section 2516 of Title 18, United States Code, that is, Title_____, United States Code, Sections _____, _____, and _____.[8]

3) During the course of the electronic surveillance authorized under the orders referred to above were communications which relate to allegations that (give a general description of conduct constituting offense), in that (describe the general contents of the conversations which are to be used). These communications were intercepted incidentally and in good faith during the course of the electronic surveillance which was conducted in accordance with the provisions of Chapter 119, Title 18, United States Code.

4) (if applicable) Among the evidence introduced at the trial of the case entitled _____ were recordings of communications intercepted pursuant to the authorization(s) referred to above.

5) (if applicable) On _____, the Honorable _____ entered an order finding that the interceptions made during the course of the electronic surveillance authorized pursuant to the orders referred to above were made pursuant to the provisions of Chapter 119, Title 18, United States Code.

WHEREFORE, on the basis of the allegations set forth above, applicant requests that the Court enter an Order authorizing the disclosure and use of the contents of communications intercepted pursuant to the orders referred to above and evidence derived therefrom while giving testimony under oath or affirmation in any proceeding held under the authority of the United States in

[8] Set forth a separate paragraph for each separate order authorizing the interception of communications.

connection with any prosecution for violations of Title 18, United States Code, Sections [ ].

UNITED STATES ATTORNEY

_____

Assistant United States Attorney

Section 2517(5) Order Permitting Testimonial Use of Interceptions Relating to "Other Offenses"

UNITED STATES DISTRICT COURT
_____ DISTRICT OF_____

IN THE MATTER OF THE APPLICATION	)	
OF THE UNITED STATES FOR AN ORDER	)	No._____
AUTHORIZING THE INTERCEPTION OF	)	
(WIRE/ORAL/ELECTRONIC)	)	
COMMUNICATIONS	)	

O R D E R

Application under oath having been made before me for an order pursuant to Section 2517(5) of Title 18, United States Code, by the United States by its attorney _____, Assistant United States Attorney for the _____ District of _____, an "investigative or law enforcement officer of the United States" as defined in Section 2510(7) of Title 18, United States Code, I FIND that:

1) On _____, United States District Judge _____, _____District of _____, entered an order in case no._____ authorizing Special Agents of the (identify the investigative agency/agencies) to intercept for a _____ day period (wire/oral/electronic) communications of _____, _____, _____, and others as yet unknown over (the telephones/pagers/facsimile machines bearing the number(s) _____ and _____ listed to _____, at _____, for the purpose of obtaining evidence concerning the commission of offenses specified in Section 2516 of Title 18, United States Code, that is Title 18, United States Code Sections _____, _____, and _____.[1]

2) During the period of authorized interception, (wire/oral/electronic) communications were intercepted in accordance with the provisions of Chapter 119, Title 18, United States Code, which were pertinent to the authorized objectives specified in the interception.

3) During the period of interception communications were also intercepted, in accordance with the provisions of Chapter

[1] Prepare a separate paragraph for each order.

119, Title 18, United States Code, incidentally and in good faith, which may be pertinent to a prosecution for a violation of Title 18, United States Code, Section(s) [ ] relating to (provide a description of the offense(s)).

WHEREFORE, It is ORDERED, pursuant to the provisions of Section 2517(5), Title 18, United States Code, that any person who has received, by any means authorized by Chapter 119, Title 18, United States Code, any information concerning the (wire/oral/electronic) communications intercepted pursuant to the authorizations specified in paragraph(s) 1, __, and __ above, or evidence derived therefrom, may disclose and use the contents of said communications, and evidence derived therefrom, while giving testimony under oath or affirmation in any proceeding held under the authority of the United States in connection with a prosecution for a violation of Title 18, United States Code, Section(s) [ ].

Date:_____

_____
UNITED STATES DISTRICT COURT JUDGE

Inventory Application

UNITED STATES DISTRICT COURT
_____ DISTRICT OF _____

_____
)
IN THE MATTER OF THE APPLICATION)
OF THE UNITED STATES OF AMERICA)
FOR AN ORDER AUTHORIZING THE)
INTERCEPTION OF WIRE[1] COMMUNICATIONS)
TO AND FROM TELEPHONE NUMBER ( ))
_____, SUBSCRIBED TO BY)
_____ and located at)
_____.)
_____)

LIST OF PERSONS NAMED IN AUTHORIZATION ORDERS
AND OTHERS WHOSE WIRE COMMUNICATIONS WERE INTERCEPTED

In order to assist the Court in making its determination of those persons to be served with inventories as provided by Title 18, United States Code, Section 2518(8)(d) in the above matter, the Government respectfully submits this compilation of the names of those persons named in the applications and court orders and other persons who have been identified by the (name the investigative agency/agencies) as persons whose wire communications were intercepted:

1. The persons named in the application and orders are:
(name) (address)

2. The persons whose wire communications were intercepted and who have been identified by the (name the agency/agencies) are:

See attached list.

3. In addition to the persons specified above, numerous communications of persons as yet unidentified were intercepted.

[1] This is just an example; inventory notice must also be sent to those individuals whose oral and electronic communications were intercepted.

In the event that any such persons are later identified, a supplemental list will be submitted to the Court.

Dated:

_____

Assistant United States Attorney

Order for Inventory

UNITED STATES DISTRICT COURT
_____ DISTRICT OF _____

_____
)
IN THE MATTER OF THE APPLICATION)
OF THE UNITED STATES OF AMERICA)
FOR AN ORDER AUTHORIZING THE)
INTERCEPTION OF WIRE COMMUNICATIONS)
TO AND FROM TELEPHONE NUMBER)
( ) _____, SUBSCRIBED TO)
BY _____ AND LOCATED AT)
_____.)
_____)

ORDER AND INVENTORY

TO: ATTORNEYS OF THE UNITED STATES DEPARTMENT OF JUSTICE

Having examined the Government's list of (a) persons named in the captioned applications and orders authorizing the interception of wire communications and (b) others thus far identified as persons whose wire communications were intercepted pursuant to those orders, pursuant to Title 18, United States Code, Section 2518(8)(d),

IT IS HEREBY ORDERED that attorneys for the United States Department of Justice shall cause to be served upon the persons listed on the annexed list an inventory which shall include notice of:

1. The fact of the entry of the orders described above authorizing the interception of wire communications.

2. The fact that the period of authorized interception pursuant to those orders included the periods between _____ and _____, 20__, and _____ and _____, 20___, by on or about which date all original recordings were sealed by order of this court.

3. The fact that during the period of authorized interception, wire communications were or were not intercepted.

The persons to be served are set forth on the attached list.

_____

UNITED STATES DISTRICT JUDGE

Inventory Notice

UNITED STATES DISTRICT COURT
_____ DISTRICT OF _____

_____
)
IN THE MATTER OF THE APPLICATION)
OF THE UNITED STATES OF AMERICA)
FOR AN ORDER AUTHORIZING THE)
INTERCEPTION OF WIRE COMMUNICATIONS)
TO AND FROM TELEPHONE NUMBER)
( )_____, SUBSCRIBED TO BY)
_____ AND LOCATED AT)
_____.)
_____)
_____)

TO: THE ADDRESSEE HERETO
PLEASE TAKE NOTICE OF THE FOLLOWING:

1. On _____, 20___ and _____, 20___, the Honorable _____ authorized the interception of wire communications over the above-captioned telephone.

2. The period of authorized interception pursuant to those orders included the periods between _____ and _____, 20__, and _____ and _____, 20___, by on or about which date all original recordings were sealed by order of this Court.

3. During the period of authorized interception, wire communications to or from your telephone were intercepted (and/or your wire communications were intercepted).

Dated:

_____
(INVESTIGATIVE AGENCY)

Application for Destruction of Tapes

UNITED STATES DISTRICT COURT
_____ DISTRICT OF _____

IN THE MATTER OF THE	)
APPLICATION OF THE UNITED	)
STATES FOR AN ORDER	)
AUTHORIZING THE DESTRUCTION	)
OF INTERCEPTED WIRE, ORAL	)
AND/OR ELECTRONIC COMMUNICATIONS	)

APPLICATION

_____, an attorney of the United States Department of Justice or (Assistant United States Attorney) states:

I am an "investigative or law enforcement officer of the United States" within the meaning of 18 U.S.C. § 2510(7), that is, an attorney authorized by law to prosecute violations of federal law.

I am also an "attorney for the government" as defined in Rule 1(b)(1) of the Federal Rules of Criminal Procedure and, therefore, pursuant to 18 U.S.C. §§ 2516(1) and (3), and 2518(8)(a), am authorized to make application to a federal judge of competent jurisdiction for authorization to destroy the original tapes of wire, oral and/or electronic communications seized pursuant to a lawful court order, in compliance with 18 U.S.C. 2518(8)(a).

This application seeks authorization to destroy the original tapes of wire, oral and/or electronic communications of (name the interceptee(s)) relating to felony violations of federal law, that is violations of (characterize the offenses) which were intercepted pursuant to a court order issued by Judge _____ of this court on the _____ day of _____ 20__.

Extensions of said order were issued on _____. The order was terminated on the _____ day of _____ 20__. The tapes herein were sealed pursuant to the order of the court on the _____ day of _____ 20__.

The tapes were subsequently unsealed pursuant to court order on the _____ day of _____ 20 _____, in connection with the (name of the prosecution or other reason for unsealing). The tapes were resealed pursuant to court order on the _____ day of _____ 20__.

(Use the following language as appropriate.)

1. The wire communications were intercepted over telephone number _____ located at _____ and subscribed to by _____.

2. Electronic communications were intercepted over (describe the facility/facilities) listed in the name of _____ and located at _____.

3. Oral communications were intercepted at (specify the location) owned or leased by _____.

(Use the following language as appropriate.)

At the time of sealing, Judge _____ ordered (identify the custodial agency) to maintain custody of the intercepted communications.

A period of ten years has elapsed since the tapes were sealed by order of Judge _____. According to my knowledge, information and belief, all prosecutions in connection therewith are terminated and there is no further need or legal reason to maintain the tapes. The investigating agency involved, (name of the agency), concurs in this application.

On the basis of the facts set forth in this application, the applicant requests that the court issue an order authorizing the destruction of the wire, oral and/or electronic communications described herein.

I declare under penalty of perjury pursuant to 28 U.S.C. § 1746 that the foregoing is true and correct to the best of my knowledge, information and belief.

Executed on the _____ day of _____ 20__.

_____

Applicant

Order for Destruction of Tapes

UNITED STATES DISTRICT COURT
_____ DISTRICT OF _____

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES FOR AN ORDER AUTHORIZING THE DESTRUCTION OF INTERCEPTED WIRE, ORAL AND/OR ELECTRONIC COMMUNICATIONS	)

ORDER AUTHORIZING THE DESTRUCTION OF INTERCEPTED WIRE, ORAL AND/OR ELECTRONIC COMMUNICATIONS

Application under penalty of perjury having been made before me by _____, an "investigative or law enforcement officer" as defined in 18 U.S.C. § 2510(7) and an "attorney for the government" as defined in Rule 1(b)(1) of the Federal Rules of Criminal Procedure, for an order authorizing the destruction of intercepted wire, oral and/or electronic communications, intercepted pursuant to.18 U.S.C. § 2510 et seq. and full consideration having been given to the matters set forth herein, the court finds:

On the _____ day of _____ 20__, an order for the interception of wire, oral, and/or electronic communications was issued by Judge _____ of this district to intercept the communications of (identify the principal person(s) and others) (over telephone number _____ located at _____ and subscribed to by _____) or (at the premises described as _____ and owned by or leased to _____) (If electronic communications were intercepted, a description of the facilities, the subscriber and the location should be set forth.) in connection with violations of _____ (specify the principal federal statutory violations). Extensions of the original order were issued on (specify the dates) by (identify the judge). The interceptions were terminated on the _____ day of _____ 20__. The intercepted communications were sealed by the court on the _____ day of _____ 20__.

The intercepted communications were subsequently used in the prosecution of (name the cases).

The tapes were unsealed pursuant to court order on _____ and resealed on _____ (use, if appropriate).

Ten years having elapsed from the time the tapes were originally sealed pursuant to 18 U.S.C. § 2518(8)(a), and there appearing to be no further need for their retention,

IT IS HEREBY ORDERED that the above-described intercepted wire, oral and/or electronic communications be destroyed by (identify the agency having possession), the lawful custodian designated by the issuing judge.

_____
Judge

Affidavit for Mobile Tracking Device

UNITED STATES DISTRICT COURT
_____ DISTRICT OF _____

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER AUTHORIZING THE MONITORING OF A MOBILE TRACKING DEVICE IN OR ON A _____, _____ LICENSE PLATE NUMBER ____, VEHICLE IDENTIFICATION NUMBER _____.	APPLICATION TO MONITOR A MOBILE TRACKING DEVICE (Fed. R. Crim. P. 41; 18 U.S.C. § 3117)

_____ DISTRICT OF _____, SS:

_____, being duly sworn, deposes and says that I am a Special Agent with the _____, duly appointed according to law and acting as such.

Upon information and belief, a_____, _____license plate number _____, vehicle identification number _____ ("the subject vehicle"), is presently being used in a conspiracy to (identify the offense(s)).

Your deponent further states that there is probable cause to believe that the installation of a mobile tracking device placed in or on the subject vehicle, and monitoring of the mobile tracking device, will lead to evidence of the aforementioned conspiracy to distribute narcotics as well as to the identification of individuals who are engaged in the commission of that and related crimes.

The source of your deponent's information and the grounds for his belief are as follows:

1. I have been a Special Agent with the _____ for _____ years, and am the case agent on this case. As the case agent, I am fully familiar with the facts of the case.

2. On or about _____, I learned from a reliable confidential informant ("CI") that _____ was involved in (list the offense(s)) in (location). The CI subsequently informed me that _____.

3. On _____, at approximately _____, I established a surveillance in the vicinity of _____. I observed _____ leave a building located at _____ and enter the subject vehicle.

4. A review of Department of Motor Vehicles records reveals that the subject vehicle is registered to _____.

5. The CI has stated that _____ is using the subject vehicle in connection with (describe the criminal activity). Based upon my own observations, I know that the subject vehicle is presently within the _____ District of _____.

6. In order to track the movement of the subject vehicle effectively and to decrease the chance of detection, I seek to place a mobile tracking device in or on the subject vehicle while it is in the _____ District of _____. Because _____ sometimes parks the subject vehicle in his driveway and on other private property, it may be necessary to enter onto private property in order to effect the installation of the mobile tracking device.

7. In the event that the Court grants this application, there will be periodic monitoring of the mobile tracking device during both daytime and nighttime hours for the next 10 days. In addition, the mobile tracking device may produce signals from inside private garages or other such locations not open to public or visual surveillance.

8. In accordance with 18 U.S.C. 3103a(b), I request that the Court order delay notification of the execution of the order for a period not to exceed ninety days (or some lesser period) because there is reasonable cause to believe that providing immediate notification would seriously jeopardize the investigation. It is requested that such period of delay thereafter be extended by the court for good cause shown.

WHEREFORE, your deponent respectively requests that the Court issue an order authorizing members of _____ or their authorized representatives, including but not limited to other law enforcement agents and technicians assisting in the above-described investigation, to install and remove a mobile tracking device in or on the subject vehicle; to enter onto private property to effect said installation and removal; to surreptitiously enter the vehicle to effect said installation and removal; and to monitor the signals from that tracking device, for

a period of 10 days following the issuance of the Court's order, including signals produced from inside private garages and other locations not open to the public or visual surveillance,

and signals produced in the event that the subject vehicle leaves the _____ District of _____ but remains within the United States.

_____
Special Agent

Sworn to before me this
____ day of _____, 20__

Order for Mobile Tracking Device

UNITED STATES DISTRICT COURT
_____ DISTRICT OF _____

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER AUTHORIZING THE MONITORING OF A MOBILE TRACKING DEVICE IN OR ON A _____, _____ LICENSE PLATE NUMBER ____, VEHICLE IDENTIFICATION NUMBER _____.	ORDER TO MONITOR A MOBILE TRACKING DEVICE (Fed. R. Crim. P. 41; 18 U.S.C. § 3117)

_____ DISTRICT OF _____, SS:

WHEREAS an affidavit has been presented to the Court by Special Agent _____ of the _____, and full consideration having been given to the matters set forth therein, this Court finds that there is probable cause to believe that monitoring of a mobile tracking device placed on a private vehicle described as a _____, _____ license plate number _____, vehicle identification number _____ ("the subject vehicle"), will lead to evidence of violations of (state the offenses). Therefore, it is

ORDERED, pursuant to Fed. R. Crim. P. 41 and 18 U.S.C. § 3117, that Special Agent _____ of the _____, together with other Special Agents and their authorized representatives are authorized, within ten days from the date of this order, to install in or on the subject vehicle, which is presently located in the _____ District of _____, a mobile tracking device; it is further

ORDERED that said Special Agents and their authorized representatives are further authorized to enter onto private property and surreptitiously to enter said vehicle to effect the installation and removal of the mobile tracking device; it is further

ORDERED that said Special Agents and their authorized representatives are authorized, for a period of ten days from the date of this order, to monitor the signals from the mobile tracking device, including those signals produced from inside any private garage or other location not open to public or visual surveillance, and, in the event the subject vehicle travels outside the _____ District of _____, those signals produced outside the _____ District of _____ but within the United States; and it is further

ORDERED that, in accordance with 18 U.S.C. 3103a(b), notification of the execution of this order be delayed for a period not to exceed ninety days (or some lesser period) because there is reasonable cause to believe that providing immediate notification would seriously jeopardize the investigation. Such period of delay may thereafter be extended by the court for good cause shown.

Dated:

_____
UNITED STATES MAGISTRATE JUDGE
(District)