



U.S. Department of Justice

Executive Office for United States Attorneys
Freedom of Information/Privacy Act Staff
600 E Street, N.W., Room 7300
Washington, D.C. 20530
202-616-6757 Fax 202-616-6478

Requester: Catherine Crump Request Number: 07-4138

Subject of Request: Mobile Phone Tracking (Item 1-4)/AGAC

NOV - 6 2008

Dear Requester:

Your request for records under the Freedom of Information Act/Privacy Act has been processed. This letter constitutes a reply from the Executive Office for United States Attorneys the official record-keeper for all records located in this office and the various United States Attorneys' Offices. A search of the files of the Attorney General's Advisory Committee has revealed no records responsive to items numbered 1-4 of your request.

Although I am aware that this request is the subject of ongoing litigation and that appeals are not ordinarily acted on in such situations, I am required by statute and regulation to inform you that if you consider my response to be a denial of your request, you have the right to file an administrative appeal by writing within 60 days from the date of this letter to the **Office of Information and Privacy, United States Department of Justice, 1425 New York Avenue, Suite 11050, Washington, D.C. 20530-0001**. In light of the fact that this is an interim response, I would ask that you wait until the EOUSA has issued its final response in this request before you file an appeal.

Sincerely,

Karen M. Gunnegan for
William G. Stewart II
Assistant Director

Enclosure(s)

Requester: Catherine Crump
FOIA #: 07-4138

Continuation Sheet:

Please note that your original letter has been split into nineteen separate files ("requests"), for processing purposes, depending on the nature of what you sought. Each file will have a separate Request Number (listed below), for which you will receive a separate response: 07-4120 through 07-4137.

This response is to FOIA No. 07-4138 only and does not include search results associated with the other requests listed above.



U.S. Department of Justice

Executive Office for United States Attorneys
Freedom of Information/Privacy Act Staff
600 E Street, N.W., Room 7300
Washington, D.C. 20530
202-616-6757 Fax 202-616-6478

Requester: Catherine Crump Request Number: 07-4126

Subject of Request: Mobile Phone Tracking (Item 1-4)/DDC

Dear Requester:

NOV - 6 2008

Your request for records under the Freedom of Information Act/Privacy Act has been processed. This letter constitutes an interim reply from the Executive Office for United States Attorneys, the official record-keeper for all records located in this office and the various United States Attorneys' Offices. To provide you the greatest degree of access authorized by the Freedom of Information Act and the Privacy Act, we have considered your request in light of the provisions of both statutes.

The records you seek are located in a Privacy Act system of records that, in accordance with regulations promulgated by the Attorney General, is exempt from the access provisions of the Privacy Act, 28 C.F.R. § 16.81. We have also processed your request under the Freedom of Information Act and are making all records required to be released, or considered appropriate for release as a matter of discretion, available to you. This letter constitutes a partial denial.

Enclosed please find:

- 47 page(s) are being released in full (RIF);
- 12 page(s) are being released in part (RIP);
- 7 page(s) are withheld in full (WIF).

This material is responsive to item number one (1) of your request. One of the documents included in the released material is the Order and Memorandum Opinion of United States District Court Judge Thomas F. Hogan dated August 25, 2006, in case numbers 06-0186, 187, 188, which consists of 11 pages. This document contains redactions made by the Court; therefore, these redactions are not included in the page count above. The exemption(s) cited for withholding records or portions of records are marked below. An enclosure to this letter explains the exemptions in more detail.

Section 552

Section 552a

- | | | | |
|---------------------------------|--|---|--|
| <input type="checkbox"/> (b)(1) | <input type="checkbox"/> (b)(4) | <input type="checkbox"/> (b)(7)(B) | <input checked="" type="checkbox"/> (j)(2) |
| <input type="checkbox"/> (b)(2) | <input checked="" type="checkbox"/> (b)(5) | <input checked="" type="checkbox"/> (b)(7)(C) | <input type="checkbox"/> (k)(2) |
| <input type="checkbox"/> (b)(3) | <input type="checkbox"/> (b)(6) | <input type="checkbox"/> (b)(7)(D) | <input type="checkbox"/> (k)(5) |
| _____ | <input type="checkbox"/> (b)(7)(A) | <input checked="" type="checkbox"/> (b)(7)(E) | <input type="checkbox"/> _____ |
| _____ | | <input type="checkbox"/> (b)(7)(F) | |

A review of the material revealed that 44 pages originated with another government component. **These records were found in the U.S. Attorney's Office files and may or may not be responsive to your request.** These records will be referred to the U.S. Department of Justice, Criminal Division for review and direct response to you.

Although I am aware that this request is the subject of ongoing litigation and that appeals are not ordinarily acted on in such situations, I am required by statute and regulation to inform you that if you consider my response to be a denial of your request, you have the right to file an administrative appeal by writing within 60 days from the date of this letter to the **Office of Information and Privacy, United States Department of Justice, 1425 New York Avenue, Suite 11050, Washington, D.C. 20530-0001.** In light of the fact that this is an interim response, I would ask that you wait until the EOUSA has issued its final response in this request before you file an appeal.

Sincerely,

A handwritten signature in cursive script that reads "Karen M. Ginnegan" followed by a stylized flourish.

William G. Stewart II
Assistant Director

Enclosure(s)

Requester: Catherine Crump
FOIA #: 07-4126

Continuation Sheet:

Please note that your original letter has been split into nineteen separate files ('requests'), for processing purposes, depending on the nature of what you sought. Each file will have a separate Request Number (listed below), for which you will receive a separate response: 07-4120 through 07-4138.

This response is to FOIA No. 07-4126 only and does not include search results associated with the other requests listed above.

EXPLANATION OF EXEMPTIONS

FOIA: TITLE 5, UNITED STATES CODE, SECTION 552

- (b)(1) (A) specifically authorized under criteria established by and Executive order to be kept secret in the in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order;
- (b)(2) related solely to the internal personnel rules and practices of an agency;
- (b)(3) specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;
- (b)(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;
- (b)(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;
- (b)(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;
- (b)(7) records or information compiled for law enforcement purposes, but only the extent that the production of such law enforcement records or information (A) could reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual.
- (b)(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or
- (b)(9) geological and geophysical information and data, including maps, concerning wells.

PRIVACY ACT: TITLE 5, UNITED STATES CODE, SECTION 552a

- (d)(5) information compiled in reasonable anticipation of a civil action proceeding;
- (j)(2) material reporting investigative efforts pertaining to the enforcement of criminal law including efforts to prevent, control, or reduce crime or apprehend criminals;
- (k)(1) information which is currently and properly classified pursuant to Executive Order 12356 in the interest of the national defense or foreign policy, for example, information involving intelligence sources or methods;
- (k)(2) investigatory material compiled for law enforcement purposes, other than criminal, which did not result in loss of a right, benefit or privilege under Federal programs, or which would identify a source who furnished information pursuant to a promise that his/her identity would be held in confidence;
- (k)(3) material maintained in connection with providing protective services to the President of the United States or any other individual pursuant to the authority of Title 18, United States Code, Section 3056;
- (k)(4) required by statute to be maintained and used solely as statistical records;
- (k)(5) investigatory material compiled solely for the purpose of determining suitability eligibility, or qualification for Federal civilian employment or for access to classified information, the disclosure of which would reveal the identity of the person who furnished information pursuant to a promise that his identity would be held in confidence;
- (k)(6) testing or examination material used to determine individual qualifications for appointment or promotion in Federal Government service the release of which would compromise the testing or examination process;
- (k)(7) material used to determine potential for promotion in the armed services, the disclosure of which would reveal the identity of the person who furnished the material pursuant to a promise that his identity would be held in confidence.

REQUESTER: Catherine Crump

FOIA FILE#: 07-4126

DOCUMENTS Released in Full "RIF"

25 pages

Chapter 3

Electronic Surveillance— Non-Wiretap

Robert Stabe, AUSA
Chief, Narcotics Enforcement Group
Southern District of Texas

- 3.1 Resources
 - 3.2 Overview
 - 3.3 Consensual monitoring
 - 3.4 Pen registers and trap and trace devices—generally
 - 3.5 Caller identification
 - 3.6 Cellular phones
 - 3.7 Subscriber information
 - 3.8 "Physical location" of cellular phone "telephone line"
 - 3.9 Extensions
 - 3.10 User consent to the installation of a trap and trace or pen register
 - 3.11 Suppression is generally not available as a remedy
 - 3.12 Emergency pen register and trap and trace installation
 - 3.13 Transponders and tracking devices—generally
 - 3.14 Duplicate display digital paging devices (clone pagers)
 - 3.15 Forward Looking Imaging Radar (FLIR) (thermal imaging)
 - 3.16 Cell site locator/digital analyzer (triggerfish)
 - 3.17 Video surveillance
-

3.1 Resources

- Electronic Surveillance Unit (ESU), Office of Enforcement Operations, Criminal Division, at (202) 514-6809.
-

- The ESU publishes two manuals, regularly updated and posted on USABook: the *Electronic Surveillance Manual*, <http://10.173.2.12/usao/eousa/ole/usabook/elsu>, and *Electronic Surveillance Issues*, <http://10.173.2.12/usao/eousa/ole/usabook/esis>.
- Fishman & McKenna, *Wiretapping and Eavesdropping* (2d Edition 1995).
- James G. Carr, *The Law of Electronic Surveillance* (1997).
- Annual Review of Criminal Procedure, and the parallel chapters on "Electronic Surveillance," *Georgetown Law Journal* (published each April).
- USAM 9-7.000 (Electronic Surveillance), and the Criminal Resource Manual at 27-37.
- *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (Computer Crime and Intellectual Property Section July 2002), posted on the Internet at <http://www.cybercrime.gov/s&smanual2002.htm>.
- Links to many of these publications, and an index of electronic surveillance issues, are on the USABook Electronic Surveillance page on DOJNET at <http://10.173.2.12/usao/eousa/ole/tables/subject/elsu.htm>.

3.2 Overview

Some of the most basic investigative techniques fall into the category of non-wiretap electronic surveillance. How a suspect organization or individual communicates can often illuminate the caliber and type of suspected criminal activity under investigation. Hence, an invaluable part of most drug investigations is the information developed at the beginning from phone toll records and pen register results, to clone pager and triggerfish results. In the end, such information can be the basis for a Title III wiretap as well as persuasive corroborating evidence at trial.

Electronic communications vs. wire communications vs. oral communications—who cares? The Office of Enforcement Operations (OEO) does, and you should. You need to know the difference if you want to be an effective prosecutor, and not incur any criminal or civil liability. Simply put, a wire communication is talking over the telephone, whether it is a hard-line phone, cordless phone, cellular phone or satellite phone. A wire communication would be someone speaking over one of these telephones. An oral communication is, for example, talking in your house or in your car. When you put a "bug" or hidden microphone in a house, you will intercept oral communications. Electronic communications run the gamut from messages sent to a pager to facsimile transmissions to e-mail messages from your computer. Generally, if it is not a wire or oral communication, it is probably an electronic communication. Tone only pagers (they may not exist any more) and tracking devices are excepted from the definition of electronic communications. When in doubt, call OEO.

The forms that appeared in this Chapter of the 1999 edition of *Federal Narcotics Prosecutions* have been updated, and are posted on USABook at <http://10.173.2.12/usao/eousa/ole/usabook/drug/forms>. Additional forms appear in Chapter 20 of the *Electronic Surveillance Manual*, on

USABook at <http://10.173.2.12/usao/eousa/ole/usabook/elsu/20elsu.htm>. Questions about which forms to use, and other electronic surveillance procedures, should be addressed to DOJ's Electronic Surveillance Unit, Office of Enforcement Operations, Criminal Division, at (202)-514-6809.

3.3 Consensual monitoring

westlaw query 18 +S 2511(2)(C) OR 18 +S 2511(2)(D)

Consensual monitoring can be accomplished with a variety of devices, from a microcassette recorder to new digital recorders. The classic hidden microphone (body mike) was often taped to a person's body. The microphone was wired either to a small transmitter or small tape recorder. The Nagra is a commonly used tape recorder which can record for a reasonably long period of time. The tape is unique and can only be played back by using special equipment or after transfer to a cassette tape.

Practice note. Investigative agencies now have small microphones concealed in many different objects that can be used by an undercover agent or informant. But one of the problems with a hidden transmitter is that the receiver (many times placed in an agent's car) has to be relatively close to the transmitter. Another problem is that the transmission can be blocked by buildings or other objects. If the person wearing the transmitter gets too far away or around large buildings, the recording can be poor. This problem can be solved by wearing a hidden tape recorder. One of the main problems with a hidden recorder is the inability to record long meetings because a small recorder needs a small tape. This is becoming less of a problem because many agencies now have digital recorders which can record a long conversation digitally on a computer chip. Once the conversation is over, the agency's technical agents transfer the digital information to a cassette tape. The agencies also have new digital transmitter devices that use cellular phone towers to transmit the signal. This results in a much clearer, cleaner recording.

Consensual tape recordings have been used and accepted in court for years, and their legality is not often challenged. Title 18 U.S.C. § 2511(2)(c) specifically states that "[i]t shall not be unlawful . . . 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 to the communication has given prior consent to such interception." When a law enforcement officer or government informant is a participant in a conversation and records the conversation, the recording is admissible in court. Section 2511(2)(d) permits private citizens to intercept a communication when they are a party to the conversation. Be aware that state laws vary, and that consensual recordings are illegal in certain states.

The Supreme Court has long recognized consensual monitoring and tape recording as a legitimate law enforcement tool. The Court found that since an undercover agent or informant could write down the conversation with a suspect and later testify about the conversation, the Constitution did not require a different result "if the agent instead of immediately reporting and transcribing his conversations with [a suspect], either (1) simultaneously records them with

electronic equipment which he is carrying on his person, *Lopez v. United States*, 373 U.S. 427 (1963), (2) or carries radio equipment which simultaneously transmits the conversations either to recording equipment located elsewhere or to other agents monitoring the transmitting frequency, *On Lee v. United States*, 343 U.S. 747 (1952); *United States v. White*, 401 U.S. 745, 751 (1971). See also *United States v. Caceres*, 440 U.S. 741 (1979) (follows and cites *White* and *Lopez*). It should be the rare instance where a consensually recorded conversation is not admitted into evidence. See *United States v. Font-Ramirez*, 944 F.2d 42, 47 (1st Cir. 1991); *United States v. Myers*, 692 F.2d 823, 859 (2d Cir. 1982) (both audio and video tape admissible where party to conversation consented); *United States v. Tangeman*, 30 F.3d 950, 952 (8th Cir. 1994); *United States v. Rodriguez-Garcia*, 983 F.2d 1563, 1569 (10th Cir. 1993); *United States v. Laetividal-Gonzalez*, 939 F.2d 1455, 1460-61 (11th Cir. 1991) (both audio and video tape admissible where informant consented to both).

Situations may arise where the cooperating informant cannot be found for trial, or the prosecutor makes the tactical decision not to call the informant to testify. Consensual tape recordings containing conversations between a defendant and the informant (or any unavailable witness) may still be admissible, assuming that the predicate for the admission of the tape recordings can be satisfied. See Fed. Rule Evid. 901(b)(5). The defendant's statements on the tape are admissible as statements or admissions of a party under Rule 801(d)(2)(A). The taped statements of the informant should be offered either as statements which the defendant has manifested an adoption or belief in their truth under Rule 801(d)(2)(B) or offered for the limited purpose of putting the defendant's responses in context and making those responses intelligible to the jury and recognizable as the admissions that they are. *United States v. Flores*, 63 F.3d 1342, 1358-1359 (5th Cir. 1995); *United States v. Gutierrez-Chavez*, 842 F.2d 77, 81 (5th Cir. 1988); *United States v. Smith*, 918 F.2d 1551, 1559 (11th Cir. 1990); *United States v. Tangeman*, 30 F.3d 950, 952 (8th Cir. 1994); *United States v. Davis*, 890 F.2d 1373, 1380 (7th Cir. 1989). As such, these statements are not hearsay because they are not offered for the truth of the matter asserted, Rule 801(c), or because they were adopted by the defendant, Rule 801(d)(2)(B). An appropriate limiting instruction to the jury should be given by the trial court at the time the statements are offered and in the jury instructions. Although the Sixth Amendment provides that a defendant has a right to be confronted with the witnesses against him, since the informant is not a "witness," the Confrontation Clause of the Sixth Amendment does not apply. *United States v. McClain*, 934 F.2d 822, 832 (7th Cir. 1991); *United States v. Gutierrez-Chavez*, 842 F.2d at 81 (no violation of the Confrontation Clause of the Sixth Amendment because the only incriminating statements of the informant to be taken as true are those statements which, in the judgment of the jury, were adopted by the defendant.)

Practice note. By offering the informant's statements in this fashion, it removes the informant as a "witness" for the government. *United States v. McClain*, 934 F.2d at 832. Since the informant is not a witness, the informant's credibility or bias should not be an issue before the jury. File a motion in limine requesting that the court order the defense not to question any government witnesses regarding prior convictions, payment records, etc. of the informant. While Rule 806, Federal Rules of Evidence, allows the defendant to attack the credibility of a declarant who did not testify when hearsay statements or statements defined in Rule 801(d)(2)(C), (D), or (E) are admitted into evidence, it does not apply to a situation

where the declarant's statements are not hearsay or are offered under Rule 801(d)(2)(A) or (B). *United States v. McClain*, 934 F.2d at 833 (Rule 806 does not apply to adopted statements under Rule 801(d)(2)(B)).

Caveat. See Section 11.33 of this Manual discussing *Crawford v. Washington*, ___ U.S. ___, 2004 WL 413301, *10, *11, *18-19 (March 8, 2004) (Confrontation Clause).

Practice note. When a cooperating defendant (charged or not) is willing to consent to the audio recording of telephone calls or the video recording of meetings, consider having the cooperating defendant sign a written consent, so that the consent does not become an issue if the cooperating defendant later has a change of heart. A form for this is posted on USABook at <http://10.173.2.12/usao/eousa/ole/usabook/drug/forms/401.htm>.

Caveat. The United States Attorneys' Manual lists instances where prior authorization is required (for example, when a public official is under investigation). The approvals are listed at USAM 9-2.400; see particularly those referencing the provisions of USAM Chapter 9-7.000.

Another useful investigative tool that prosecutors and agents should consider is a consensual wire intercept. Many prosecutors have experienced the situation where an informant does not record a telephone call either because the informant is not particularly good at following instructions or the informant is driving a car at the time of the call or because the informant is with a target of the investigation. Title 18 U.S.C. § 2511(2)(c) authorizes any person acting under color of law to intercept a wire or electronic communication where that person is a party to the communication or one of the parties to the communication has given prior consent to the interception. Generally, a court order is needed only because the service provider will not assist law enforcement with such an intercept unless they are provided with a court order. Such a consensual wire intercept does not require approval from the Electronic Surveillance Unit at OEO and the provisions of §§ 2516 and 2518 don't apply. This can be very effective when local agents are conducting an investigation with an informant located out of town. Instead of relying on the informant to tape record his conversations and turn the tape recordings over to an agent (in person or through the mail), agents can now record every conversation and have complete control over the recording.

Practice note. Because the intercept is lawful only when a party to the conversation has consented to the intercept, the informant needs to be briefed and strongly warned not to loan the phone to anyone. Monitors should be familiar with the informant's voice so they can minimize an intercept if they don't hear the informant as a party to a conversation. Forms for the application, order and written consent appear as Forms 302, 303, and 304 on USABook at <http://10.173.2.12/usao/eousa/ole/usabook/drug/forms>.

3.4 Pen registers and trap and trace devices—generally

westlaw query "PEN REGISTER" OR "TRAP AND TRACE"

There have been many changes to the pen register statute as a result of the Patriot Act.

A pen register, also called a dialed number recorder (DNR), is a device that records the numbers dialed from a telephone. A pen register works on the standard residential or business telephone (commonly referred to as a hard-line phone) and also a cellular telephone. Gone are the days when an agent had to climb a telephone pole or set up next door to the telephone location to hook into a phone line. Due to modern technology, a pen register can now be connected to a person's telephone line from almost anywhere. Most investigative agencies have rooms at their office where they can set up and monitor pen registers. There are situations where agencies may monitor a telephone in New Jersey from a pen register in New York or monitor a telephone in Laredo from a pen register located in Houston.

A pen register is activated every time the telephone is picked up (off hook). A pen register records every number or symbol that is dialed. If a person dials an 800 pager with a PIN and sends a callback number followed by a code number to the pager, a pen register will record all the numbers dialed. The number may look something like this: 1-800-567-90001234567132221234*300#. Looking at this, you could see that 1-800-567-9000 is an 800 pager, that the PIN is 123456, the callback number is 713-222-1234 and the caller used a code of 300. This was the type of information that a pen register could provide. The gathering and use of this information is now limited by amendments to the statute and DOJ policy.

Practice note. The technology used in pen registers can also be used to intercept conversations. If a pen register is operating on a telephone, and a court authorizes a wiretap on that telephone, a technical agent only has to flip a switch to start monitoring the conversation.

A trap and trace used to be limited to a process conducted by the local telephone company. Caller ID is a trap and trace device. Since the advent of caller ID, most people are familiar with a trap and trace device and have one installed on their telephone. A trap and trace provides the telephone number calling a particular telephone. The traditional trap and trace requires the local telephone company to perform the trace and provide the information to the investigative agency. This is still done in some investigations and can provide useful information. It is becoming much more common for investigative agencies to request that Caller ID be activated on a target telephone, if it is not already activated by the customer. This allows the pen register to record the originating telephone number and provides an agent with real-time information rather than waiting for a response from the telephone company a day or more later.

In the landmark case discussing pen register devices, *Smith v. Maryland*, 442 U.S. 735 (1979), the Supreme Court rejected the defendant's claim that he had a legitimate expectation of privacy in the numbers dialed on his telephone. *Id.* at 742. The Court said that even if the defendant had such an expectation of privacy, it was not one that society was prepared to recognize as reasonable. *Id.* at 743. On this basis, the Court held that the installation and use of a pen register was not a search under the Fourth Amendment and that no warrant was required to install or use a pen register. *Id.* at 745-46.

Though the Supreme Court held in *Smith* that use of a pen register did not violate constitutional rights, federal statutes require law enforcement officials to obtain a court order

before installing or using either a pen register or a trap and trace device. See Title 18, Chapter 206, set forth in 18 U.S.C. §§ 3121-3127. Since the Patriot Act, Chapter 206 has been extensively amended (a redline and strikeout version illustrating the changes is on USABook at <http://10.173.2.12/usao/eousa/ole/usabook/patr/pentrap.htm>). It is broken down into seven sections:

- **Title 18 U.S.C. § 3121** contains the general prohibition on installing or using a pen register or trap and trace device, establishes exceptions for law enforcement and service providers, and sets out the penalty provisions for violating this statute. The limitation subsection was amended and now requires that a government 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.” 18 U.S.C. § 3121(c).
- **Title 18 U.S.C. § 3122** sets forth the requirements for an application seeking court authorization to install or use a pen register or trap and trace device.
- **Title 18 U.S.C. § 3123** sets forth the requirements for a court order authorizing the installation or use of a pen register or trap and trace device, including the issuance and content of the order, the time period for the order (60 days maximum) and the time period and condition precedent for extensions (60 days maximum for each extension, provided that for each extension the court makes the finding required in connection with the original application), sealing the order and non-disclosure by service providers and others. There have been several amendments to this subsection. 18 U.S.C. § 3123(a)(1) broadens the reach of the order by stating that the court shall issue an order for “anywhere within the United States” and including language that the court’s order shall apply to any person or entity providing wire or electronic communication service whose assistance may facilitate the execution of the court’s order. Another amendment removed the requirement that the court order specify the geographic limits of the trap and trace device when an attorney for the government makes the application. 18 U.S.C. § 3123(b)(1)(C). If a state law enforcement officer makes an application for a trap and trace device, the court order must still specify the geographic limits of the device.
- **Title 18 U.S.C. § 3124** (and 18 U.S.C. § 3123(b)(2)) concerns assistance by service providers and others, including compensation.
- **Title 18 U.S.C. § 3125** concerns emergency pen register and trap and trace installations.
- **Title 18 U.S.C. § 3126** concerns reports by the Attorney General to Congress.
- **Title 18 U.S.C. § 3127** defines terms, such as “pen register,” “trap and trace device,” “wire communication,” “electronic communication,” “electronic communication service,” “court of competent jurisdiction” and “attorney for the government.”

The definition of a pen register in 18 U.S.C. § 3127(3) has been amended by the Patriot Act, and is defined as:

the term 'pen register' means 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

This new definition allows a pen register on an e-mail account in order to gather the e-mail header information of messages sent to the target e-mail account. Under the new definition, it is clear that the information from a pen register can not include the contents of any communication. The new definition for a trap and trace device also contains the same language regarding e-mail accounts and the same language excluding the contents of any communication. "Contents" includes any information concerning the substance, purport, or meaning of that communication. 18 U.S.C. § 2510(8).

Note. Section 216 of the Patriot Act redefined a "court of competent jurisdiction," which now means any federal district or magistrate court having jurisdiction over the offense being investigated. 18 U.S.C. § 3127(2). This amended definition allows a federal court in a district with jurisdiction over the offense under investigation to authorize a pen register or trap and trace device in any other district, regardless of the location of the telephone or facility, and the application need only establish that the authorizing court has jurisdiction over the offense under investigation. When dealing with an e-mail account, the physical location of the pen register or trap and trace device will generally be the location of the internet service provider's equipment. Without the change in the statute, government attorneys, agents and magistrate judges in jurisdictions where internet service providers are located would have been inundated with such requests.

The application for a pen register or trap and trace device must include:

1. The identity of the government attorney making the application;
2. The identity of the law enforcement agency conducting the investigation;
3. If known, the identity of the subscriber(s) of the telephone to which the pen register or trap and trace device will be attached. Title 18 U.S.C. § 3123(b)(1)(A) uses the phrase "the identity . . . of the person to whom is leased or in whose name is listed the telephone";
4. If known, the "identity . . . of the person who is the subject of the criminal investigation;"
5. The "number" of the telephone to which the pen register or trap and trace device will be attached. If the target phone is a cellular telephone, the application should:
 - (a) clearly state that the target phone is a cellular telephone, and,
 - (b) identify the phone by its electronic serial number (ESN) or International Mobile Subscriber Identification (IMSI) number;
6. If known, the "physical location of the telephone line" to which the pen register or trap and trace device will be attached; and,
7. The offense(s) to which the information likely to be obtained relates.

The application should also contain a certification by the government attorney "that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted" by the named law enforcement agency *and* be made "in writing and under oath or equivalent affirmation to a court of competent jurisdiction." See 18 U.S.C. §§ 3122-23.

If the application satisfies § 3122, then the court *shall* issue an ex parte order authorizing the installation and use of the pen register or trap and trace device. 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). "Section 3123(a) requires only confirmation by the court that identification [of the official applying] and certification [by that official] have occurred." *In re Application of the United States for an Order Authorizing the Installation and Use of a Pen Register and Trap and Trace Device*, 846 F.Supp. 1555, 1559 (M.D. Fla. 1994); see also *United States v. Fregoso*, 60 F.3d 1314, 1320 (8th Cir. 1995)(holding that the judicial role under § 3123(a) is ministerial in nature because a proper application under § 3122 mandates entry of the order). There is no requirement for a showing of probable cause because the installation and use of a pen register is not a search. See *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.") The Magistrate Judge reviewing an application for a pen register or trap and trace device should only determine if the statutory requirements have been met. "[T]he extremely limited judicial review required by 18 U.S.C. § 3122 is intended merely to safeguard against purely random use of this device by ensuring compliance with the statutory requirements established by Congress." *United States v. Hallmark*, 911 F.2d 399, 402 (10th Cir. 1990). If the application satisfies § 3122, then the court *shall* issue an ex parte order authorizing the installation and use of the pen register and/or trap and trace device anywhere within the United States.

In light of § 3123, as well as other considerations, the court order should:

1. Set forth:
 - (a) the name of the attorney for the government making the application;
 - (b) a finding that the "attorney for the government has certified to the court that the information likely to be obtained by the installation and use of the pen register or trap and trace device is relevant to an ongoing criminal investigation; and
 - (c) the name of the law enforcement agency identified in the application;
2. Authorize the installation and use of a pen register and/or trap and trace device;
3. Specify, if known, the identity of the subscriber(s) of the telephone to which the pen register and/or trap and trace device will be attached;
4. Specify, if known, the "identity . . . of the person who is the subject of the criminal investigation";

5. Specify the "number" of the telephone to which the pen register and/or trap and trace device will be attached;

Note. If the target phone is a cellular telephone, the application should clearly state that the target phone is a cellular telephone and identify the phone by its electronic serial number (ESN) or International Mobile Subscriber Identification (IMSI) number;

6. Specify, if known, the "physical location of the telephone line" to which the pen register and/or trap and trace device will be attached;

7. State the "offense" to which the information likely to be obtained relates;

8. Contain a direction to the service provider or other person to furnish, upon request of the applicant (the government attorney), "information, facilities, and technical assistance necessary to accomplish the installation or use of the pen register and/or trap and trace device under Section 3124 [of Title 18]";

9. Authorize the capture of the pen register and/or trap and trace information by whatever means is reasonably necessary to effectuate the order; and,

10. Contain a direction that the order is sealed until otherwise ordered by the Court;

11. Contain a direction to the service provider or other person not to disclose the existence of the pen register and/or trap and trace device or the existence of the investigation to the listed subscriber or to any other person, unless and until otherwise ordered by the Court.

Even before the enactment of the Patriot Act, the physical location of a telephone did not control which federal court had authority to order a pen register or trap and trace with respect to that telephone. A federal court had jurisdiction to authorize a pen register or trap and trace in two instances:

1. When the target telephone was physically located within its district; *or*

2. When the pen register or trap and trace was monitored within its district—even if the target telephone was physically located outside the district.

United States v. Denman, 100 F.3d 399 (5th Cir. 1996); see also *In re Application of the United States for an Order Authorizing the Installation and Use of a Pen Register and Trap and Trace Device*, 846 F.Supp. at 1562; *United States v. Burford*, 755 F. Supp. 607, 611 (S.D.N.Y. 1991).

As part of the Patriot Act, Congress amended 18 U.S.C. § 3121(c) so that it now requires that a governmental agency "authorized to install and use a pen register or trap and trace device . . . shall 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 to not include the contents of any wire or electronic communications." Unlike the 1994 amendment, this provision applies to both pen registers and trap and trace devices. It compels something analogous to "minimization" when the technology to do so is "reasonably available." Congress intended that, when practicable, the pen register and trap and trace device would solely capture processing and transmitting information. Using the example above, if a pen register recorded

1-800-567-90001234567132221234*300#, the statute would limit the government to the number of the pager, 1-800-567-9000 and, arguably, the PIN (123456). While the PIN is not necessary for processing the actual call, the PIN is necessary to route the call to the particular pager. Neither the callback number, 713-222-1234, nor the code, 300, are necessary for processing the call, and clearly are communicating information to the recipient.

On May 24, 2002, Deputy Attorney General Larry Thompson issued a memorandum entitled, "Avoiding Collection and Investigative Use of 'Content' in the Operation of Pen Registers and Trap and Trace Devices" (on the Internet at <http://www.house.gov/judiciary/87238.PDF> and on DOJNET at <http://10.173.2.12/usao/eousa/ole/tables/misc/penreg.pdf>). This memorandum sets forth the Department of Justice's policy regarding avoidance of "overcollection" in the use of pen registers and trap and trace devices. The original definition of a pen register and trap and trace device involved a device which recorded the numbers transmitted on the telephone line. By this definition, a pen register was permitted to capture all the numbers dialed or transmitted from a particular telephone. The Patriot Act not only amended 18 U.S.C. § 3121(c) but also amended the definition of a pen register and trap and trace device. Both amendments make the legislative intent clear that the content of any communication should not be intercepted if at all possible. It is the position of OEO that technology is still not reasonably available to limit a pen register or trap and trace device to only the numbers dialed for call processing. For example, to place a long distance call using a telephone calling card, one might dial 18009991111987654123456787135672233. All these numbers are necessary for call processing, that is, for the call to be placed. The first set of numbers, 1-800-999-1111, accesses the long distance carrier. The second set of numbers, 987 654 1234 5678, is the calling card account number. The last set of numbers, 713-567-2233, is the actual telephone number being called. This is what is referred to as "post-cut-through digits." "Post-cut-through digits" are any digits that are dialed from a telephone after the initial call setup is completed. For example, "[s]ome 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." *United States Telecom Association v. FCC*, 227 F.3d 450, 462 (D.C. Cir. 2000). 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. At other times "post-cut-through digits" can also represent call content, as discussed in the pager example above (other examples are account numbers when a person calls an automated banking service or passwords when calling a voice-mail system).

Caveat. Technology is available to limit the pen register device so that it only records a specified number of dialed digits, for example, the first 10 digits. While this may eliminate the inadvertent collection of the "content" of a communication (referred to as "overcollection"), it may also eliminate the collection of legitimate, lawful data pertinent to an investigation.

Deputy Attorney General Thompson's memorandum states there shall be no affirmative investigative use of any "content." Prosecutors need to be aware of this policy and should check with the agency operating the pen register to determine what steps the agency has taken to either limit overcollection or limit the use of content. Prosecutors must insure that information/data gathered as a result of overcollection is not used in affidavits, court filings or to further the investigation.

Pen registers cannot be used to collect Uniform Resource Locators (URLs), commonly referred to as web addresses, without prior consultation with the Computer Crime and Intellectual Property Section (CCIPS) of the Criminal Division. See USAM 9-7.500.

3.5 Caller identification

*westlaw query "CALLER ID!" & 18 +S 312**

Installation and use of a caller identification device (Caller ID) falls within the definition of a trap and trace device and is governed by the requirements of 18 U.S.C. §§ 3122 and 3123. See 18 U.S.C. § 3127(4) (defining "trap and trace device"); *United States v. Fregoso*, 60 F.3d 1314, 1320 (8th Cir. 1995). The statute no longer requires that the court order specify the geographical limits of a trap and trace device unless a state law enforcement officer is the applicant. See 18 U.S.C. § 3123(a)(1) & (2). With Caller ID, it is usually not possible to limit its function to certain areas. In those limited circumstances where a geographic limit needs to be specified, it appears that the statute does not require that there be an actual limit, simply that the limitation be specified. Specifying that the limits of Caller ID are within the geographical limits of the United States should satisfy the statute and is consistent with telephone technology.

Caveat. When Caller ID is ordered as part of a trap and trace request, the telephone company activates that feature for the particular telephone. If the subject of the investigation—during the course of the interception—purchases a Caller ID box and connects it to his telephone, the Caller ID box will work despite the fact that he is not subscribing to the Caller ID service. This may alert the subjects to the fact that they are under investigation.

3.6 Cellular phones

westlaw query "CELL! PHONE" /P 18 +S 3127(3)

Prior to the enactment of the Patriot Act, it was the position of the Electronic Surveillance Unit, of DOJ's Office of Enforcement Operations, that a court order was *not* required if the interception will solely capture the electronic serial number of a cellular telephone.

Under Section 216 of the Patriot Act, the new definition of pen register in 18 U.S.C. § 3127(3) includes a device 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." Based on this new definition, a pen register order must be

secured before the use of a digital analyzer ("triggerfish") to capture the electronic serial number of a cellular telephone.

3.7 Subscriber information

westlaw query "SUBSCRIBE!" /P 18 +S 2703(C)

A variety of procedures to obtain information about subscribers whose numbers are recorded by a pen register or a trap and trace are set forth in 18 U.S.C. § 2703(c)(1). For example, 18 U.S.C. § 2703(c)(1) & (2) provides for access by warrant, by court order, by subscriber consent, and by subpoena. To obtain subscriber-type information *by court order* under that section, the application will need to include "specific and articulable facts showing that there are reasons 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 investigation." 18 U.S.C. § 2703(d).

The substance and numbering of § 2703 was amended by the Patriot Act. Section 2703(c)(1)(C) is now § 2703(c)(2). Section 2703(c)(2) provides a more detailed listing of the subscriber information and records that may be sought by a governmental entity. A service provider shall disclose the following information for a subscriber or customer:

- (A) name;
- (B) address;
- (C) local and long distance telephone connection records, or records of session times and durations;
- (D) length of service (including start date) and types of service utilized;
- (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and,
- (F) means and source of payment for such service (including any credit cards or bank account number)

When a governmental entity receives any of the records listed above, the governmental entity is not required to notify the subscriber or customer. 18 U.S.C. § 2703(c)(3) ("[a] governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.").

Title 18 U.S.C. § 2703(b) can be used to acquire the content of opened e-mail. Section 2703 sets forth the standards for government-compelled disclosure of a customer's electronic communications held by a provider. It differentiates between communications in "electronic storage" for less than 180 days, and communications held by a "remote computing service" and describes the legal process required to compel disclosure of each. Under § 2703(a), disclosure of communications in "electronic storage" (unopened e-mail, for example) for 180 days or less may be compelled only by means of a warrant; however, disclosure of communications stored with a "remote computing service" (opened e-mail) may be compelled by means of a court order.

Practice note. The Computer Crime and Intellectual Property Section (CCIPS) of DOJ provided an excellent memorandum for presentation to a federal judge explaining the law and the difference between unopened e-mail and opened e-mail. A version of that memorandum along with a sample application and order are posted on USABook at <http://10.173.2.12/usao/eousa/ole/usabook/drug/forms> (Forms 315-317). For a more detailed explanation, see Chapter III (The Electronic Communications Privacy Act), Sections B, C, and D, of *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, prepared by CCIPS and revised in July 2002, posted on the Internet at http://www.cybercrime.gov/s&smanual2002.htm#_IIIB_.

When requesting any type of information other than records or subscriber information under § 2703(c), a non-disclosure order must be obtained. To obtain a statutory non-disclosure order applicable to content information furnished under 18 U.S.C. § 2703, the application must state facts establishing "that there is reason to believe that notification of the existence of the . . . court order will result in: (1) endangering the life or physical safety of an individual; (2) flight from prosecution; (3) destruction of or tampering with evidence; (4) intimidation of potential witnesses; or (5) otherwise seriously jeopardizing an investigation or unduly delaying a trial." 18 U.S.C. § 2705(b). One way to provide such factual information to the court would be to have a law enforcement officer act as affiant on an appropriate affidavit and for that affidavit to be made an attachment to the prosecutor's application. Another way is for the applicant to recite the information in the application and attribute it to an agent or agency.

The forms found on USABook at <http://10.173.2./usao/eousa/ole/usabook/drug/forms> can be used when requesting a pen register and/or trap and trace device (and/or Caller ID)—with or without subscriber information. Use Forms 313 and 314 for those situations when subscriber information alone is sought (under 18 U.S.C. § 2703).

Alternatively, as noted above, under 18 U.S.C. § 2703(c)(2), subscriber-type information may also be obtained by administrative subpoena, grand jury subpoena, trial jury subpoena, or search warrant.

3.8 "Physical location" of cellular phone "telephone line"

Title 18 U.S.C. § 3123(b) requires that the order for pen register and/or trap and trace shall specify the "number" and "if known," the "physical location of the telephone line to which the pen register or trap and trace device is to be attached." According to the Criminal Division's Office of Enforcement Operations, care should be taken when requesting either a pen register or a trap and trace on a cellular phone:

1. The application papers (and proposed order) should clearly state that the target phone is a cellular phone;
2. The application papers (and proposed order) should, whenever possible, identify the phone by either its electronic serial number (ESN) or International Mobile Subscriber Identification (IMSI) number, *and* the manufacturer's identification number (MIN) (telephone number); and

3. The proposed order should authorize the capture of the pen register information and/or trap and trace information by whatever means is reasonably necessary to effectuate the order.

3.9 Extensions

westlaw query 18 +S 3122(C) /P EXTEN!

The time period for the order is a maximum of 60 days. 18 U.S.C. § 3122(c). That same subsection sets forth the time period and condition precedent for extensions: 60 days maximum for each extension, provided that for each extension the court again makes the finding required in connection with the original application.

3.10 User consent to the installation of a trap and trace or pen register

The Criminal Division's Office of Enforcement Operations takes the position that, where the "user" of a telephone consents to the installation of a trap and trace or pen register, the "consent" provision in 18 U.S.C. § 3121(b)(3) obviates the need for a court order. The statute is less than clear on this point, because subsection (b)(3) appears directed to the "service provider," not a law enforcement agency. *Compare* 18 U.S.C. § 3121(b)(3) with 18 U.S.C. § 3121(c). Further, it will still be necessary to obtain subscriber-type information on the phone numbers recorded by the pen register or trap and trace. *See, e.g.*, 18 U.S.C. § 2703(c).

3.11 Suppression is generally not available as a remedy

westlaw query 18 +S 3121(A) & "EXCLUSIONARY RULE"

As set forth above, as a general rule, to legally install or use a pen register or a trap and trace, one must first obtain a court order under 18 U.S.C. § 3121-3127. A "knowing" violation of the statute can trigger criminal sanctions. *See* 18 U.S.C. § 3121(d). However, the statute does *not* prescribe suppression of evidence as a remedy for its violation; nor is a violation of the statute, in and of itself, a violation of a constitutional right. *United States v. Thompson*, 936 F.2d 1249, 1252 (11th Cir. 1991) ("Implementation of a judicially imposed exclusionary remedy for a violation of these congressionally mandated [pen register] procedures would be out of proportion to the infraction. . . . Absent either a constitutional or statutory basis for excluding the evidence obtained through this [pen register] procedure, the district court correctly denied the motion to suppress.").

3.12 Emergency pen register and trap and trace installation

The statute authorizes certain law enforcement officials to authorize the installation and use of a pen register and trap and trace—without a court order—when "an emergency situation exists that involves—

- (A) immediate danger of death or serious bodily injury to any person, or
- (B) conspiratorial activities characteristic of organized crime."

See 18 U.S.C. § 3125. However, depending on the circumstances, it may be quicker to obtain judicial authorization (or, if available, "user" consent) to install a pen register or trap and trace, than to obtain emergency authority from the law enforcement officials specified in the statute. Moreover, unless a state has the requisite enabling legislation, the statute does not confer upon the officials of that state power to authorize an emergency pen register or trap and trace. See 18 U.S.C. § 3125(a).

3.13 Transponders and tracking devices—generally

westlaw query "EXPECTATION OF PRIVACY" /P "TRACKING DEVICE" OR
TRANSPONDER

Tracking devices have progressed a long way. Most agencies now have sophisticated tracking devices that use cell site towers or satellites. These tracking devices are either battery operated or wired into the vehicle's electrical system (after securing a court order). The tracking devices are similar to the anti-theft car devices now being marketed (Lo-Jac) that help the police locate your stolen car, and the in-car devices (On Star) that show drivers their location on a computer displayed map. These types of tracking devices are usually monitored from the law enforcement agency's office. Through the use of computers, a signal is sent to the tracking device (it is pinged), and the tracking device responds. The signal is picked up using cellular telephone cell sites or satellites. The location of the tracker, and therefore the vehicle, is determined through triangulation and a computer monitor at the agency office shows the location of the vehicle on a map. These tracking devices are very accurate, and can differentiate between a vehicle traveling on an interstate highway or the feeder (service) road. The tracking devices will also provide the direction of travel and the speed the vehicle is traveling.

The use of tracking devices is generally governed by case law, not statute. In many instances, the use of a tracking device is simply to assist law enforcement in conducting physical surveillance. In these circumstances, there is no reasonable expectation of privacy and the Fourth Amendment does not apply. There is no search or seizure in violation of the Fourth Amendment when law enforcement authorities monitor a tracking device placed in a car because "a person traveling in an automobile on a public thoroughfare has no reasonable expectation of privacy in his movements from one place to another." *United States v. Knotts*, 460 U.S. 276, 281 (1983).

Similarly, there is no Fourth Amendment violation when law enforcement authorities monitor a tracking device placed in a boat traveling on the open seas, *United States v. Juda*, 46 F.3d 961, 968 (9th Cir. 1995), or placed in an airplane flying in public airspace, *United States v. Butts*, 729 F.2d 1514, 1517 (5th Cir. 1984) (*en banc*).

This does not mean that law enforcement officials have carte blanche to use tracking devices. The Fourth Amendment does apply to tracking devices in certain situations. The only statute that specifically addresses mobile tracking devices is 18 U.S.C. § 3117. This statute states that "if a court is empowered to issue a warrant or other order for the installation of a mobile tracking device, such order may authorize the use of that device . . . outside that jurisdiction if the device is installed in that jurisdiction." Section 3117 presumes a court has the power to issue an order for the installation of such a device. *United States v. Gbemisola*, 225 F.3d 753, 757 n. 2 (D.C. Cir. 2000), cert. denied, 531 U.S. 1026 (2000); *In Re Application of the United States*, 155 F.R.D. 401, 403 (D. Mass. 1994). Before § 3117 was enacted, courts historically relied on Rule 41, Fed. R. Crim. P., for the authority to issue orders regarding the installation of tracking devices. *Id.*

In *United States v. Karo*, 468 U.S. 705 (1984), the Supreme Court divided its analysis of the use of a tracking device into two parts: (1) installation, and (2) monitoring.

- **Installation.** Where DEA agents placed a monitoring device in a container of chemicals with the consent of the chemical company and prior to delivery of the chemicals to the customer/suspect, the Court found no Fourth Amendment violation. *Id.* at 711. The logical result from the *Karo* decision is if the tracking device is going to be placed within a vehicle or object without the consent of the owner, a warrant or court order will have to be obtained based upon a showing of probable cause. The particularity requirement of the Fourth Amendment is satisfied if the affidavit includes a description of the object into which the tracking device is to be placed, the circumstances and facts that caused the agents to request the use of the tracking device, and the length of time that the tracking device will be installed and monitored. *United States v. Karo*, 468 U.S. at 718. Even before the *Karo* decision, the Ninth Circuit Court of Appeals found a court order necessary for agents to enter a private garage, open the hood of a truck and attach a tracking device to the battery under the hood. *United States v. Hufford*, 539 F.2d 32, 34 (9th Cir. 1976). No court order is needed, though, to install a tracking device on the exterior of a car while parked in a public place. *United States v. Michael*, 645 F.2d 252, 256 (5th Cir. 1981) (*en banc*).
- **Monitoring.** If a tracking device assists agents in learning the same information they could have from visual surveillance, then, in general, no court order is needed to monitor the tracking device. *United States v. Knotts*, 460 U.S. at 282. This is so even if the agents were not actually conducting the surveillance. This is the rationale behind the decisions regarding cars, boats and airplanes on or in public roads, water and air.

If the tracking device conveys information that "could not have been visually verified," then a warrant is needed to monitor the tracking device. *United States v. Karo*, 468 U.S. at 715. The monitoring of a tracking device falls within the ambit of the Fourth Amendment when it reveals a "critical fact about the interior" of a location that could not have been obtained through visual surveillance. *Id.* at 715-16. The Court notes that "warrants for the installation and monitoring

of a beeper will obviously be desirable since it may be useful, even critical, to monitor the beeper to determine that it is actually located in a place not open to visual surveillance." *Id.* at 713 n. 3. For example, detecting the movement of a package from the trunk of a car parked inside an attached garage (and no longer visible from the outside) to a room of the house through the use of a hidden tracking device would require a court order to monitor it. In this example, this movement could not have been detected from surveillance agents outside the house.

No warrant or court order is needed to place a tracking device in a package containing contraband, stolen property or the like because the individual possessing such an item has no legitimate expectation of privacy in items that the individual has no right to possess at all. *United States v. Gbemisola*, 225 F.3d at 759; *United States v. Moore*, 562 F.2d 106, 111 (1st Cir. 1977); *United States v. Washington*, 586 F.2d 1147, 1154 (7th Cir. 1978); *United States v. Jones*, 31 F.3d 1304, 1310-11 (4th Cir. 1994).

Practice note. Seek a court order in most cases. Some districts present a request for a mobile tracking device using the application for a search warrant and search warrant forms. Read the *Knotts* and *Karo* decisions. For an extensive analysis of the *Knotts* and *Karo* decisions read *Electronic Tracking Devices and the Fourth Amendment: Knotts, Karo and the Questions Still Unanswered*, 34 Cath. U. L. Rev. 277 (Winter 1985). A sample application can be found on USABook at <http://10.173.2.12/usao/eousa/ole/usabook/drug/forms/418.htm>. Since the basis of a mobile tracking device order is Rule 41, the revised sample application/order incorporates the language of Title 18, U.S.C. § 3103a(b), which provides for delayed notice of the execution of a search warrant.

3.14 Duplicate display digital paging devices (clone pagers)

westlaw query "CLONE PAGER"

A clone pager is a pager provided to an agent by the pager company that is identical to the target pager (hence the name "clone"). The clone pager then receives every page that the target pager receives (ideally). This requires an agent to always carry the clone pager. Some investigative agencies secure the access codes from the pager company and program a computer to capture the pages going to the target pager.

Practice note. Even with the computer system, agents still receive a duplicate pager and carry it as a backup (there are times when the computer system fails). This also frees up an agent for other duties who would otherwise have to constantly monitor the computer at the office.

Practice note. With the low cost and ease of acquiring cellular telephones, the use of pagers seems to be declining. Using the Text Messaging option on cellular telephones is becoming more commonplace. Check with the cellular telephone service provider to determine if a particular cellular telephone has Text Messaging capabilities. Pen registers can differentiate between dialed calls and Text Messages, so have the case agent check with the agency tech

agents. Text Messages fall under the definition of an electronic communication, and a Title III must be secured, with the approval of OEO, to intercept Text Messages in real time.

Practice note. The use of Nextel's push-to-talk feature (radio) is also becoming much more popular. Pen registers can show if an individual is using the push-to-talk feature. This can aid you in securing an intercept order for these conversations although, in many areas, technology is not available to allow the interception of push-to-talk conversations. Check with the tech agent for the investigative agency.

Securing a clone pager allows an agent to intercept and monitor the numbers and messages that are sent to that particular pager. Oftentimes, these messages are the call-back telephone numbers, but the messages may also include partial numbers (your target knows the entire number), meeting times, meeting locations, drug prices, and drug quantities.

Unfortunately, without a wire intercept at the same time, these coded messages may not be easily understood. There have been circumstances where an individual will discuss putting in the price per kilo of cocaine and the clone pager message will reflect "165" for \$16,500, or an individual will discuss putting in an amount of cocaine, and the clone pager message will reflect "54" for 54 packages of cocaine. *See United States v. Broussard*, 80 F.3d 1025 (5th Cir. 1996). Circumstances have also been found where the targets of an investigation have agreed upon several meeting locations that are assigned numbers, and a message to meet at a particular location can be sent via a pager by simply sending the number of the location and a time. All of this is to say that clone pagers can provide a variety of good intelligence information and can also establish links between co-conspirators.

Congress saw fit to treat clone pagers the same as wire intercepts under 18 U.S.C. §§ 2510-2522. The rationale was that the government was intercepting messages sent to the pager, not just numbers dialed as in a pen register. As with a wire intercept, similar requirements must be met in order to secure authorization to intercept electronic communications. That is, the affidavit must establish probable cause to believe the pager is being used in the offense(s) listed, the need for the interception, and must describe the success or lack thereof of alternative investigative techniques. Because of this, the application, affidavit and orders for the interception of electronic communications are similar to those forms used to apply for an interception of wire communications.

Even though the forms are similar, there are some differences between wire and oral interceptions and the interception of electronic communications, such as:

- While § 2516(1) of Title 18 describes specific offenses in which a wire or oral intercept can be authorized, § 2516(3) states that the interception of electronic communications can be authorized for any federal felony offense;
- Authorization from a Deputy Assistant Attorney General is not required to intercept electronic communications (see Title 18 U.S.C. § 2516(3)). The Department of Justice also does not require prior approval for a clone pager. USAM 9-7.114. Each United States Attorney's Office should have a procedure in place for approval of interceptions involving clone pagers. Prior approval by the Department of Justice is required for all other

interceptions involving electronic communications, such as facsimile transmissions, teletype communications, Text Messaging, e-mail, or computer transmissions. *Id.*

- Section 2518(10)(a) of Title 18, which describes the grounds for a motion to suppress wire or oral interceptions, does not apply to electronic communications. Subsection (10)(c) states that the remedies and sanctions regarding the interception of electronic communications described in the statute are the only judicial remedies and sanctions for non-constitutional violations. Practically speaking, this leaves very few remedies to a defendant trying to suppress evidence from the interception of electronic communications. In addition, the good faith exception of *United States v. Leon*, 468 U.S. 897 (1984), applies to interception cases. *United States v. Moore*, 41 F.3d 370, 376 (8th Cir. 1994). Subsection (d), the sealing requirement of section 2518(8)(a), does apply to electronic communications. Failure to timely seal the records could cause the results of the interception of electronic communications to be suppressed. *United States v. Rios*, 495 U.S. 257 (1990).

Forms and samples for applications, affidavits and orders can be found on USABook at <http://10.173.2.12/usao/eousa/ole/usabook/drug/forms> (Forms 321-324). Records are generated as a result of the interception of a pager. Some law enforcement offices have the capability to capture and store in a computer the messages sent to a clone pager, in which case there is a computer printout that lists each and every message intercepted. In other situations, the agent monitoring the clone pager must write down the messages as they are received in the clone pager. In either case, a record is made and it is suggested that this record (either computer generated or hand written) be presented to the court for sealing. In *United States v. Suarez*, 906 F.2d 977 (4th Cir. 1990), the court found no violation of the sealing requirement because there were no recordings to seal. This case involved the use of a clone pager where the monitoring officers recorded by hand the messages that were intercepted. The Fourth Circuit Court of Appeals affirmed the district court's ruling that there was no recording by a device comparable to a tape recorder, so the sealing requirement was never triggered. *Id.* at 982-83. The court's rationale was that the recording and sealing requirement is designed to protect the integrity of the intercepted conversations/messages. The court reasoned that recording intercepted messages by hand does not protect the "recording" from editing or alteration; in fact, recording by hand makes alteration possible.

Practice note. Unless you are interested in making law in your circuit, seal the records, whether kept by computer or by hand. It does not take very long, and saves you from at least one legal argument.

Practice note. Depending on the pager and the telephone company, a trap and trace can be placed on a pager telephone number. A trap and trace on a pager will provide agents with the number of the telephone that is calling the pager telephone number. This is *all* it should do. A trap and trace on a pager will not and should not register the message sent to the pager. If it does, it is an unlawful interception of electronic communications. Just like a trap and trace device on a telephone line, it can provide agents with telephone numbers that help identify co-conspirators and their locations and can assist in developing probable cause for a clone pager affidavit.

3.15 Forward Looking Imaging Radar (FLIR) (thermal imaging)

westlaw query "THERMAL IMAG!" OR INFRARED /P MARIJUANA

Thermal imaging devices have been used often in marijuana growing and harvesting investigations. Thermal imaging involves using a device, usually from an airplane, that measures the heat radiating from an object. The object is usually a house or other structure on a suspect's property. If the scan reveals an inordinate amount of heat being radiated, it is an indication of, and consistent with, the use of indoor lights associated with marijuana cultivation. This information is usually incorporated into a search warrant for the property.

Although a majority of circuits *had* ruled that obtaining a thermal image of a suspect's residence or property did not constitute a search and that a search warrant was not required, the Supreme Court found otherwise. In a 5-4 decision, the Supreme Court reversed the Ninth Circuit decision in *Kyllo v. United States*, 533 U.S. 27, 34-35 (2001), finding that "obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical intrusion into a constitutionally protected area constitutes a search." Such a search is "presumptively unreasonable without a warrant." *Id.*, 533 U.S. at 40. Since the Supreme Court decision in *Kyllo*, an agent must obtain a search warrant before using a thermal imaging device.

It appears that thermal imaging may still be used with the curtilage of a house or a commercial structure. If the thermal imaging device is used from an aircraft, as is commonly done, the aircraft should be in public airspace and complying with FAA regulations regarding altitude. See *California v. Ciraolo*, 476 U.S. 207 (1986) (overflight of individual's backyard from airplane *lawfully* operating at an altitude of 1,000 feet does not violate the Fourth Amendment); *Dow Chemical Co. v. United States*, 476 U.S. 227, 229 (1986) (overflight of industrial complex from airplane *lawfully* operating at altitudes of 12,000, 3,000 and 1,200 feet does not violate the Fourth Amendment); *Florida v. Riley*, 488 U.S. 445 (1989) (overflight of individual's backyard from a helicopter *lawfully* operating at an altitude of 400 feet does not violate the Fourth Amendment).

Note. The Supreme Court noted in *Florida v. Riley* that "[w]e would have a different case if flying at that altitude had been contrary to law or regulation." 488 U.S. at 451. Make sure the airplane or helicopter complies with federal laws and FAA regulations regarding proper altitude or your evidence could get suppressed.

3.16 Cell site locator/digital analyzer (triggerfish)

A "triggerfish" or "swamp box" is a device that can intercept signals from a cellular telephone. This device has also been referred to as a digital analyzer and ESN reader. FCC regulations require all cellular telephones to contain an Electronic Serial Number, commonly referred to as the ESN. The ESN is electronically programmed in every telephone by chips and/or software.

The Mobile Identification Number (MIN) is the actual telephone number for that cellular telephone. When a user turns on (powers up) a cellular telephone, the cellular telephone transmits the identity of the phone to the nearest cell site. The transmitted information is the ESN/MIN. These numbers allow the cellular system to identify the particular telephone and allow the cellular company to bill that particular telephone for the air-time charges. A cellular telephone that is powered up is exchanging this information with cell sites even though no call is in progress.

A "triggerfish" device can perform several functions. A "triggerfish" can intercept this identifying signal and "read" the Electronic Serial Number and Mobile Identification Number of the cellular telephone. From a law enforcement standpoint, if a law enforcement officer has a target that uses a cellular telephone, the officer can use a "triggerfish" to determine the ESN/MIN of the cellular telephone being used by the target. Once a law enforcement officer knows the ESN or MIN, a subpoena can be issued to all the cellular telephone companies in the area requesting the subscriber information and air-time billing records for that particular cellular telephone.

Based on Section 216 of the Patriot Act (pen register definition), it is the opinion of the Electronic Surveillance Unit, Office of Enforcement Operations, that a pen register order is required to intercept the electronic serial number of a cellular telephone. The amended definition includes "signaling information transmitted by an instrument" and includes such information as the ESN signal.

A "triggerfish" can also record the numbers dialed from a particular cellular telephone. If used in this way, the "triggerfish" meets any definition of a pen register and a pen register order must be obtained. With very little additional effort, the "triggerfish" can also intercept the conversations taking place on a particular cellular telephone. If used in this way, the "triggerfish" is intercepting wire communications and a wire intercept order is required; wiretaps are covered in Chapter 4 of this Manual.

A "triggerfish" can also be used to determine the cell site being used by a particular cellular telephone. In addition, the cellular telephone company should be able to provide cell site information. Once a cell site is determined, law enforcement agents can conduct surveillance in a more specific area in an effort to identify the user of the cellular telephone.

Practice note. See pen register forms (305-308) on USABook at <http://10.173.2.12/usao/eousa/ole/usabook/drug/forms>.

3.17 Video surveillance

westlaw query "VIDEO SURVEILLANCE" & "EXPECTATION OF PRIVACY"

The use of video surveillance is governed by case law and not statute in domestic criminal investigations. As with hidden tape recordings, an undercover agent, informant or any individual may consent to videotaping a meeting or conversation with a hidden camera. *United States v. Laetividal-Gonzalez*, 939 F.2d 1455, 1460 (11th Cir. 1991).

Law enforcement authorities may place hidden cameras in a position so that the cameras view areas open to the public. For example, a camera monitoring the front of a house, apartment or business, a parking area, a lobby area or hallway is generally permitted without court authorization. See USAM 9-7.210. In some of these examples, the owner of the property would have to consent to the placement of the camera.

If law enforcement authorities want to place a hidden camera so that they can monitor and record activities in an area where there is a reasonable expectation of privacy, a court order must be secured. This is considered a search, and Rule 41 of the Federal Rules of Criminal Procedure applies. Since the basis for installing and monitoring a hidden video camera is Rule 41, revised 18 U.S.C. § 3103a(b) now applies. Forms 325-327 on USABook at <http://10.173.2.12/usao/eousa/ole/usabook/drug/forms> have been revised to include delayed notice language. Unlike a traditional search which is limited in its intrusion, a hidden video camera can record for hours, days, and months if approved by a court. The courts have stepped in and set out the requirements for securing a court order to install and monitor a hidden video camera in an area where there is a reasonable expectation of privacy. The four generally accepted requirements are:

1. The judge issuing the order must find that normal investigative techniques have been tried and have failed or reasonably appear unlikely to succeed if tried or appear to be too dangerous to try;
2. The order must contain a particular description of the type of activity sought to be intercepted and a statement of the particular offense(s) to which it relates;
3. The order must not allow the period of interception to be longer than is necessary to achieve the objective of the investigation or, in any event, no longer than thirty days;
4. The order must require that the interception be conducted in such a way as to minimize the interception of activities not related to the offense under investigation.

United States v. Biasucci, 786 F.2d 504, 510 (2d Cir. 1986); *United States v. Cuevas-Sanchez*, 821 F.2d 248, 252 (5th Cir. 1987); *United States v. Torres*, 751 F.2d 875, 883-84 (7th Cir. 1984); *United States v. Falls*, 34 F.3d 674, 680 (8th Cir. 1994); *United States v. Koyomejian*, 970 F.2d 536, 542 (9th Cir. 1992) (*en banc*) (*Koyomejian II*); *United States v. Mesa-Rincon*, 911 F.2d 1433, 1437 (10th Cir. 1990) (specifically added fifth requirement of probable cause to believe that a particular person is committing, has committed or is about to commit a crime).

These four requirements may sound like the requirements to intercept a wire or oral communication, because the courts looked to 18 U.S.C. §§ 2510-2522 to fashion these requirements. The Department of Justice also requires that any application/orders for video surveillance should include a particularized description of the premises to be surveilled, and the names of the persons to be surveilled, if known. USAM 9-7.230. Prior to applying to a court for an order to conduct video surveillance, the application, affidavit and order must be approved by either an Assistant Attorney General, Deputy Assistant Attorney General, the Director of the Office of Enforcement Operations or the Associate Director of the Office of Enforcement Operations. USAM 9-7.210. Commonly, the Director or Associate Director of the Office of

Enforcement Operations authorizes the application. Submit the application through the Electronic Surveillance Unit of OEO.

Practice note. If you are applying for authorization to install a listening device (bug) inside some structure, you should also apply for authorization to install a camera. If you have probable cause to justify the listening device, you should have probable cause to justify the installation of a camera. This will enhance your case and also make identification of the speakers much easier if you also have them on video.

The forms for an application, affidavit and order for video surveillance are posted on USABook at <http://10.173.2.12/usao/eousa/ole/usabook/drug/forms> (Forms 325-327).

Pen Register Request Form

TO: Carolyn Carter-McKinley (202-616-3389 Fax 202-616-2296)

FROM: AUSA Name: _____
(Please print the way you would like it to appear in signature block)

Bar Number: _____

Name of SA/Officer: _____ Agency: _____

Telephone and Cell/Pager Number(s): _____

RE: Title of Investigation: _____ USAO # (required): _____

Brief description of criminal activity:

U.S. Code Violation(s): _____

Number and Type of Telephone (Land or Cell): _____

Name and address of Subscriber: _____

If cell, provide ESN/IMSI/IMEI #: _____ Service Provider: _____

If *subscriber* information is desired, please give a brief specific factual statement of the reasons subscriber information is relevant and material to the investigation:

If cell site *information* is desired, please give a brief statement setting forth reasons why cell site location information will be relevant and material to the investigation:

REQUESTER: Catherine Crump

FOIA FILE#: 07-4126

MIXED DOCUMENTS

Pages RIF 22

Pages RIP 12

Pages WIF _____

DUP Pages _____

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE APPLICATION)
OF THE UNITED STATES OF AMERICA)
FOR AN ORDER AUTHORIZING) MISC. NO. _____
DISCLOSURE OF SUBSCRIBER AND CELL)
SITE INFORMATION ON CELLULAR) UNDER SEAL
TELEPHONE NUMBER [INSERT NUMBER])

APPLICATION FOR DISCLOSURE OF SUBSCRIBER AND CELL SITE
INFORMATION PURSUANT TO TITLE 18 U.S.C. SECTION 2703

The United States of America, by and through its counsel, Kenneth L. Wainstein, United States Attorney for the District of Columbia, and [INSERT NAME OF AUSA], Assistant United States Attorney, hereby applies to the Court for an order directing [INSERT NAME OF SERVICE PROVIDER] (hereinafter "Service Provider"), an electronic communications service provider for the telephone number [INSERT TELEPHONE NUMBER] (hereinafter "subject cellular telephone number"), a cellular telephone with the [INSERT APPROPRIATE IDENTIFICATION NUMBER, E.G. ESN, IMSI, etc.], subscribed to by [INSERT NAME AND ADDRESS OF SUBSCRIBER], to disclose to the [INSERT NAME OF AGENCY] (hereinafter "Agency") subscriber information relating to telephone numbers called from and calling to the subject cellular telephone, and cell site information relating to the subject telephone. In support of this application, the United States certifies the following:

1. The Applicant is an "attorney for the government" as defined in Rule 1(b)(1) of the Federal Rules of Criminal Procedure.

2. The Applicant certifies that the Agency is conducting a criminal investigation of the user(s) of the subject cellular telephone number and others in connection with possible violations of federal laws, including [INSERT CODE CITATIONS]. Based upon reliable information, it is believed that the user(s) of subject cellular telephone number, subscribed to by [INSERT NAME AND ADDRESS OF SUBSCRIBER], utilizes the cellular telephone in violation of [INSERT CODE CITATIONS]. [INSERT A BRIEF DESCRIPTION OF CRIMINAL ACTIVITY].

3. The Applicant further certifies that there is reasonable grounds to believe that the requested subscriber and cell site information is relevant and material to the ongoing criminal investigation being conducted by the Agency. As set forth more fully below, it is believed this information will provide the agents with investigative leads and potential evidence at trial concerning contacts made by the targets in the course of their criminal activity.

SUBSCRIBER INFORMATION

4. In an accompanying Application, the Applicant has requested that the Court issue an order authorizing the use of a pen register/trap and trace device to register numbers dialed to or pulsed from the subject cellular telephone number.

5. In this Application, the Applicant further requests, pursuant to Title 18 U.S.C. Section 2703(c)(1)(B), the use of a caller identification device on the subject cellular telephone and that for each telephone number for which they possess such information the Service Provider, and any other provider of electronic communication service, be directed to provide to the Agency the subscriber information, including subscriber name and address, telephone location, length of service, as well as all information regarding the means and source of payment for service for all telephone numbers dialed or pulsed from the subject cellular telephone number, as indicated by the pen register, and all telephone numbers calling the subject cellular telephone number, as indicated by the trap and trace and caller identification device, whether published or non-published.¹

6. In support of its request for an order under Title 18 U.S.C. Section 2703(d), directing the disclosure of subscriber information, the Government hereby sets forth the following specific and articulable facts showing that there is reasonable grounds to believe that the requested subscriber information will be relevant

¹ (

[t

ME

ME

ME
ME

]

and material to an ongoing criminal investigation for the following reasons:

7. [INSERT BRIEF SPECIFIC FACTUAL STATEMENT SETTING FORTH REASONS WHY SUBSCRIBER INFORMATION IS RELEVANT AND MATERIAL TO THE INVESTIGATION].

CELL SITE INFORMATION

8. The Applicant further requests, pursuant to Title 18 U.S.C. Sections 2703(c)(1)(B) and (d), that the Service Provider listed in the accompanying proposed order, 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 be issued, disclose any records showing the location of cell site/sector (physical address) at call origination (for outgoing calls), and call termination (for incoming calls) if reasonably available.

9. Cell site information will be of great assistance to the investigation to ascertain the area in which the target phone is located when calls are being made.

10. The Applicant requests further that the Court's Order direct the Service Provider, its agents, employees and affiliates not to disclose to the subscriber, or to any other person, the disclosure of information requested herein unless or until otherwise ordered by the Court.

11. It is further requested that the Court's Order apply not only to the subject cellular telephone number, but also to [

b7E
b7E
b7E
b7E
b7E
b7E
b7E

] which are listed to the same

subscriber and wireless telephone account number as the subject cellular telephone number within the 60 day period authorized by this Order.

12. It is further requested that the Court's Order apply to the Service Provider, and to any other communications service provider which contracts or otherwise agrees to provide cellular telephone service to a telephone bearing the same telephone number or [INSERT APPROPRIATE IDENTIFICATION NUMBER, E.G. ESN, IMSI, etc.] during the sixty day period authorized by this Order.

13. Because disclosure of this Application could jeopardize the investigation for which the authorization to disclose subscriber and cell site information is sought, the Applicant further requests that this Application be filed under seal. The Applicant further

requests that this Court's Order, and any subsequent orders, be sealed until otherwise ordered by the Court.

WHEREFORE, it is respectfully requested that the Court grant an Order for a period of 60 days directing the Service Provider, or any other electronic communications provider subject to the Court's Order, to disclose to the Agency subscriber and cell site information relating to the subject cellular telephone number, and sealing this Application and the Court's Order.

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

EXECUTED on this _____ day of _____, 2005.

Respectfully submitted,

KENNETH L. WAINSTEIN
UNITED STATES ATTORNEY
DC Bar No. 451-058

[INSERT NAME OF AUSA]
ASSISTANT UNITED STATES ATTORNEY
555 4th Street, NW
Washington, DC 20001
DC BAR NO. [AUSA'S BAR NUMBER]
[INSERT AUSA'S TELEPHONE NUMBER]

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE APPLICATION)
OF THE UNITED STATES OF AMERICA)
FOR AN ORDER AUTHORIZING) MISC. NO. _____
DISCLOSURE OF SUBSCRIBER AND CELL)
SITE INFORMATION ON CELLULAR) UNDER SEAL
TELEPHONE NUMBER [INSERT NUMBER])

ORDER

This matter having come before the Court pursuant to the Government's Application under Title 18 U.S.C. Section 2703, by [INSERT NAME OF AUSA], an attorney for the government, which Application requests an Order under Title 18 U.S.C. Section 2703, authorizing the installation of a caller identification device, on [INSERT TELEPHONE NUMBER] (hereinafter "subject cellular telephone number"), a cellular telephone, [INSERT APPROPRIATE IDENTIFICATION NUMBER, E.G. ESN, IMSI, etc.], subscribed to by [INSERT NAME AND ADDRESS OF SUBSCRIBER], and directing the disclosure of subscriber records and cell site information pertaining to the subscriber, the Court makes the following findings:

Findings Pursuant to Title 18 U.S.C. Section 2703(d)

1. There are reasonable grounds to believe that the contents of the requested records, subscriber information and cell site information are relevant and material to an ongoing criminal investigation described in the Application; accordingly,

ORDER

IT IS ORDERED, pursuant to Title 18 U.S.C. Section 2703, that agents of the [INSERT NAME OF AGENCY] (hereinafter "Agency") may install and use a caller identification device on the subject cellular telephone, for a period of sixty (60) days; and

IT IS FURTHER ORDERED, pursuant to Title 18 U.S.C. Sections 2703(c)(1)(B) and 2703(d), that for each telephone number for which they possess such information, [INSERT NAME OF SERVICE PROVIDER] (hereinafter "Service Provider"), and any other provider of electronic communication service, shall provide to the Agency all subscriber information, including subscriber name and address, telephone location, and length of service, as well as all information regarding the means and source of payment for service, for all telephone numbers dialed or pulsed from the subject cellular telephone number, as indicated by the pen register, and all telephone numbers calling the subject cellular telephone number, as indicated by the trap and trace and caller identification device, whether published or non-published, and

IT IS FURTHER ORDERED, pursuant to Title 18 U.S.C. Section 2703(d) that the Service Provider shall provide cell site/sector (physical address) at call origination (for outgoing calls), and call termination (for incoming calls), and if reasonably available, during the progress of the call, and

IT IS FURTHER ORDERED, that this Order shall apply not only to the subject cellular telephone number, but also to [

b7E
b7E
b7E
b7E
b7E
b7E
b7E
b7E]

which are listed to the same subscriber and wireless telephone account number as the subject cellular telephone number within the 60 day period authorized by this Order.

IT IS FURTHER ORDERED, that this Order shall apply to the Service Provider, and to any other service provider which contracts or otherwise agrees to provide cellular telephone service to a telephone bearing the same telephone number and/or [INSERT APPROPRIATE IDENTIFICATION NUMBER, E.G. ESN, IMSI, etc.] during the 60 day period contemplated by the Order in this matter.

IT IS FURTHER ORDERED, that the Service Provider, or any other service provider to whom this Order applies, shall be compensated by the Agency for reasonable expenses incurred in providing technical assistance; and

IT IS FURTHER ORDERED, that this Order and the Application shall be sealed until otherwise ordered by the Court and that the Service Provider, its agents, employees and affiliates, shall not disclose the existence of the caller identification device or the existence of the investigation to the listed subscriber, or to any other person, unless or until otherwise ordered by the Court.

SO ORDERED this _____ day of _____, 2005.

UNITED STATES MAGISTRATE JUDGE

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE APPLICATION)
OF THE UNITED STATES OF AMERICA)
FOR AN ORDER AUTHORIZING) MISC. NO. _____
DISCLOSURE OF AND CELL SITE)
INFORMATION ON CELLULAR) UNDER SEAL
TELEPHONE NUMBER [TELEPHONE NUMBER])

APPLICATION FOR DISCLOSURE OF CELL SITE INFORMATION
PURSUANT TO TITLE 18 U.S.C. SECTION 2703

The United States of America, by and through its counsel, Kenneth L. Wainstein, United States Attorney for the District of Columbia, and [INSERT NAME OF AUSA], Assistant United States Attorney, hereby applies to the Court for an order directing [INSERT SERVICE PROVIDER] (hereinafter "Service Provider"), an electronic communications service provider for the telephone number [INSERT CELLULAR TELEPHONE NUMBER] (hereinafter "subject cellular telephone number"), a cellular telephone with the [INSERT APPROPRIATE IDENTIFICATION NUMBER, E.G. ESN, IMSI, etc.], subscribed to by [INSERT NAME AND ADDRESS OF SUBSCRIBER] to disclose to [INSERT NAME OF AGENCY] (hereinafter "Agency") cell site information relating to the subject telephone. In support of this application, the United States certifies the following:

1. The Applicant is an "attorney for the government" as defined in Rule 1(b)(1) of the Federal Rules of Criminal Procedure.
2. The Applicant certifies that the Agency is conducting a criminal investigation of the user(s) of the subject cellular

telephone number and others in connection with possible violations of federal laws, including [INSERT CODE CITATIONS]. Based upon reliable information, it is believed that the user(s) of subject cellular telephone number, subscribed to by [INSERT NAME AND ADDRESS OF SUBSCRIBER], utilizes the cellular telephone in violation of [INSERT CODE CITATION], [INSERT A BRIEF DESCRIPTION OF CRIMINAL ACTIVITY].

3. The Applicant further certifies that there is reasonable grounds to believe that the requested cell site information is relevant and material to the ongoing criminal investigation being conducted by the Agency. As set forth more fully below, it is believed this information will provide the agents with investigative leads and potential evidence at trial concerning contacts made by the targets in the course of their criminal activity.

CELL SITE INFORMATION

4. The Applicant requests, pursuant to Title 18 U.S.C. Sections 3122, 3123, and 2703(c)(1)(B) and (d), as set forth in the accompanying Application of [INSERT NAME OF AUSA] for a Pen Register, Caller Identification and Cell Site Information Pursuant to Title 18 U.S.C. Sections 3122 and 3133, which Application is adopted and incorporated by reference herein, that the Service Provider listed in the accompanying proposed order, 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 be issued, disclose the location of cell site/sector (physical address) at call origination (for outgoing calls), call termination (for incoming calls) and if reasonably available, during the progress of a call.

5. The cell site information that the Government seeks to obtain on a prospective basis is information that ordinarily would be obtained by a "pen register device" as defined in Title 18 U.S.C. Section 3127, and is also "records or other information" as defined in Title 18 U.S.C. Section 2703(c). As such "records or other information" the cell site information's disclosure is obtainable by a court issuing an order that complies with Title 18 U.S.C. Section 2703(d), as well as with Title 18 U.S.C. Section 3123.¹ An order can issue under Section 2703(d) only upon a finding that the information is both "relevant and material" to an ongoing investigation. For the following reasons, it is reasonable to

¹ As is our practice, the Government is seeking to acquire cell site information pursuant to both Title 18 U.S.C. Sections 3122, 3123, and Title 18 U.S.C. Section 2703(b)(1)(C) and (d). In order to comply with the July 25, 2005 Order of the Magistrate Judges of this Court, we have invoked the authority of the two controlling statutes in separate applications, each of which is incorporated by reference into the other.

believe that the cell site information sought in this Application will be both relevant and material to the ongoing investigation.

6. [INSERT BRIEF STATEMENT SETTING FORTH REASONS WHY CELL SITE LOCATION INFORMATION WILL BE RELEVANT AND MATERIAL TO THE INVESTIGATION]

7. The Applicant requests further that the Court's Order direct the Service Provider, its agents, employees and affiliates not to disclose to the subscriber, or to any other person, the disclosure of information requested herein unless or until otherwise ordered by the Court.

8. It is further requested that the Court's Order apply not only to the subject cellular telephone number, but also [b7E

[b7E
b7E
b7E
b7E
b7E
b7E]

[b7E] which are listed to the same subscriber and wireless telephone account number as the subject cellular telephone number within the 60 day period authorized by this Order.

9. It is further requested that the Court's Order apply to the Service Provider, and to any other communications service provider which contracts or otherwise agrees to provide cellular telephone

service to a telephone bearing the same telephone number or [INSERT TYPE OF IDENTIFICATION NUMBER] during the sixty day period authorized by this Order.

10. Because disclosure of this Application could jeopardize the investigation for which the authorization to disclose subscriber and cell site information is sought, the Applicant further requests that this Application be filed under seal. The Applicant further requests that this Court's Order, and any subsequent orders, be sealed until otherwise ordered by the Court.

WHEREFORE, it is respectfully requested that the Court grant an Order for a period of 60 days directing the Service Provider, or any other electronic communications provider subject to the Court's Order, to disclose to the Agency subscriber and cell site information relating to the subject cellular telephone number, and sealing this Application and the Court's Order.

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

EXECUTED on this ____ day of _____, 2005.

Respectfully submitted,

KENNETH L. WAINSTEIN
UNITED STATES ATTORNEY
DC Bar No. 451-058

[INSERT NAME OF AUSA]
ASSISTANT UNITED STATES ATTORNEY
555 4th Street, NW
Washington, DC 20001
DC BAR NO. [AUSA'S BAR NUMBER]
[INSERT AUSA'S TELEPHONE NUMBER]

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE APPLICATION)
OF THE UNITED STATES OF AMERICA)
FOR AN ORDER AUTHORIZING) MISC. NO. _____
DISCLOSURE OF AND CELL SITE)
INFORMATION ON CELLULAR) UNDER SEAL
TELEPHONE NUMBER [TELEPHONE NUMBER])

ORDER

This matter having come before the Court pursuant to the Government's Application under Title 18 U.S.C. Section 2703, by [INSERT NAME OF AUSA], an attorney for the government, which Application requests an Order under Title 18 U.S.C. Section 2703, authorizing the installation of a caller identification device, on [INSERT TELEPHONE NUMBER] (hereinafter "subject cellular telephone number"), a cellular telephone, [INSERT TYPE OF IDENTIFICATION NUMBER, E.G. ESN, IMSI, ETC., AND ACTUAL NUMBER], subscribed to by [INSERT NAME AND ADDRESS OF SUBSCRIBER], and directing the disclosure cell site information pertaining to the subscriber, the Court makes the following findings:

Findings Pursuant to Title 18 U.S.C. Section 2703(d)

1. There are reasonable grounds to believe that cell site information is relevant and material to an ongoing criminal investigation described in the Application; accordingly,

ORDER

IT IS ORDERED, pursuant to Title 18 U.S.C. Section 2703, that agents of the [INSERT NAME OF AGENCY] (hereinafter "Agency") may install and use a caller identification device on the subject cellular telephone, for a period of sixty (60) days; and

IT IS FURTHER ORDERED, pursuant to Title 18 U.S.C. Section 2703(d) that the Service Provider shall provide cell site/sector (physical address) at call origination (for outgoing calls), and call termination (for incoming calls), and if reasonably available, during the progress of the call, and

IT IS FURTHER ORDERED, that this Order shall apply not only to the subject cellular telephone number, but also to [b7E]

[b7E
b7E
b7E
b7E
b7E
b7E
b7E]

[b7E] which are listed to the same subscriber and wireless telephone account number as the subject cellular telephone number within the 60 day period authorized by this Order.

IT IS FURTHER ORDERED, that this Order shall apply to the Service Provider, and to any other service provider which contracts or otherwise agrees to provide cellular telephone service to a telephone bearing the same telephone number and/or INSERT TYPE OF IDENTIFICATION NUMBER, E.G. ESN, IMSI, ETC.] during the 60 day period contemplated by the Order in this matter.

IT IS FURTHER ORDERED, that the Service Provider, or any other service provider to whom this Order applies, shall be compensated by the Agency for reasonable expenses incurred in providing technical assistance; and

IT IS FURTHER ORDERED, that this Order and the Application shall be sealed until otherwise ordered by the Court and that the Service Provider, its agents, employees and affiliates, shall not disclose the existence of the caller identification device or the existence of the investigation to the listed subscriber, or to any other person, unless or until otherwise ordered by the Court.

SO ORDERED this ____ day of _____, 2005.

UNITED STATES MAGISTRATE JUDGE

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE)
APPLICATION OF THE UNITED)
STATES OF AMERICA FOR AN ORDER) MISC. NO. _____
AUTHORIZING THE INSTALLATION)
AND USE OF A PEN REGISTER, TRAP) UNDER SEAL
AND TRACE, AND CALLER)
IDENTIFICATION DEVICE ON CELLULAR)
TELEPHONE NUMBER [TELEPHONE NUMBER])
AND DISCLOSURE OF SUBSCRIBER AND)
CELL SITE INFORMATION)

APPLICATION FOR PEN REGISTER, CALLER
IDENTIFICATION DEVICE, SUBSCRIBER AND CELL SITE INFORMATION

The United States of America, by and through its counsel, Jeffrey A. Taylor, United States Attorney for the District of Columbia, and [INSERT NAME OF AUSA], Assistant United States Attorney, hereby applies to the Court for an Order authorizing the installation and use of a pen register, trap and trace and caller identification device on, and for subscriber information relating to, telephone numbers called from and calling to the telephone line presently assigned number [INSERT CELLULAR TELEPHONE NUMBER], a cellular telephone with the Electronic Serial Number (ESN) [INSERT ESN NUMBER] subscribed to by [INSERT NAME AND ADDRESS OF SUBSCRIBER] and authorizing disclosure of cell site information on cellular telephone number [INSERT CELLULAR TELEPHONE NUMBER]. In support of this application, the United States certifies the following:

1. The 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 Title 18, United States Code, Section 3122, may apply for an Order authorizing the installation and use of a pen register, trap and trace, and/or a caller identification device.

2. The Applicant certifies that the [INSERT NAME OF AGENCY], (hereinafter "the Agency") is conducting a criminal investigation of the user(s) of the cellular telephone identified above and others in connection with possible violations of federal laws, including [INSERT CODE CITATIONS]. Based upon reliable information, it is believed that the user(s) of cellular telephone number [INSERT CELLULAR TELEPHONE NUMBER], subscribed to by [INSERT NAME AND ADDRESS OF SUBSCRIBER], utilizes the cellular telephone in furtherance of [INSERT CODE CITATION], [INSERT A BRIEF DESCRIPTION OF CRIMINAL ACTIVITY].

3. The Applicant further certifies that the information likely to be obtained from the pen register and the caller identification device is relevant to the ongoing criminal investigation being conducted by the Agency. It is believed this information will provide the agents with investigative leads and potential evidence at trial concerning contacts made by the targets in the course of their criminal activity. The information to be obtained from the

caller identification feature is

b7E

[

b7E

b7E

b7E

]

4. The Applicant requests that the Court issue an Order authorizing the use of (1) a pen register to register numbers dialed to or pulsed from [INSERT CELLULAR TELEPHONE NUMBER], to record the date and time of such dialings or pulsings, and

b7E

[

b7E

[b7E] and (2) the use of the trap and trace and caller identification device¹ on [INSERT CELLULAR TELEPHONE NUMBER] to capture the incoming electronic and other impulses which identify the originating number of a wire or electronic communication, and the date and time of such incoming pulses, for a period of sixty (60) days.

5. The Applicant further requests that the Order direct [INSERT NAME OF SERVICE PROVIDER] to furnish all information, facilities, and technical assistance necessary to accomplish the installation of the pen register, trap and trace and the caller identification device unobtrusively with a minimum of interference

¹

(

[

b7E]

b7E

b7E

b7E

b7E

]

with the services that the provider accords the subscriber(s), and with compensation to be paid by the Agency for reasonable expenses incurred in providing such facilities and assistance.

6. The Applicant requests further that the Court's Order direct [INSERT NAME OF SERVICE PROVIDER], its agents, employees and affiliates not to disclose to the subscriber, or to any other person, the existence of the requested pen register, trap and trace, or the caller identification device, or of this investigation, unless or until otherwise ordered by the Court.

7. [INSERT LANGUAGE STATING WHY SUBSCRIBER INFORMATION REQUESTED PURSUANT TO §2703 IS RELEVANT TO THE INVESTIGATION. THE FOLLOWING LANGUAGE MAY BE USED IN NARCOTICS CASES]

The Applicant believes that the target cellular telephone is being used to facilitate drug trafficking. Subscriber information concerning telephones in contact with the target cellular telephone will assist investigators in identifying persons involved in the illegal activity. Moreover, in the experience of the Applicant and the law enforcement personnel conducting the investigation in this matter, persons engaged in illegal narcotics trafficking also are engaged in money laundering in violation of 18 United States Code, §§ 1956 and 1957. Such money laundering activity [b7E]

[b7E]

[JTE] Information concerning the means and methods by which the subscriber or user of a cellular telephone number pays for that service will provide evidence of illegal narcotics activity and related money laundering and thus assist law enforcement in the investigation of the illegal narcotics activity of the target.

8. The Applicant submits that the facts set forth in paragraphs two and seven herein provide reasonable grounds to believe that the contents of records and information relating to subscribers or customers of telephones in contact with [INSERT CELLULAR TELEPHONE NUMBER] are relevant and material to the ongoing criminal investigation. Therefore, the applicant also requests, pursuant to Title 18, United States Code, Sections 2703(c)(1)(B) and 2703(d), that for each telephone number for which they possess such information, [INSERT NAME OF SERVICE PROVIDER] and any other provider of electronic communication service, be directed to provide to the Agency the subscriber information, including subscriber name and address, telephone location, length of service, as well as all information regarding the means and source of payment for service, for all telephone numbers dialed or pulsed from [INSERT CELLULAR TELEPHONE NUMBER], as indicated by the pen register, and all telephone numbers calling [INSERT CELLULAR TELEPHONE NUMBER], as indicated by the trap and trace and caller identification device, whether published or non-published. As noted above, the

subscriber's name will be shown on the caller identification feature; however, it will not appear if the number is a non-published number.

9. In support of its request for an order under 18 U.S.C. §2703(d) directing the furnishing of cell site information pursuant to 18 U.S.C. §§ 2703(c)(1)(B) and 2703(d), the government hereby sets forth the following specific and articulable facts showing that there is reasonable grounds to believe that the cell site information regarding [INSERT CELLULAR TELEPHONE NUMBER] will be relevant and material to an ongoing criminal investigation for the following reasons:

10. [INSERT BRIEF, SPECIFIC FACTUAL STATEMENT AS TO WHY CELL SITE INFORMATION IS RELEVANT TO THE INVESTIGATION. FOR NARCOTICS CASES THE FOLLOWING STATEMENT MAY BE USED.]

Your applicant and the law enforcement personnel conducting the investigation in this matter know that persons engaged in illegal narcotics trafficking utilize their telephones to arrange meetings at which narcotics are supplied and payment for those narcotics are made. Knowing the location of the trafficker when such telephone calls are made will assist law enforcement in discovering the location of the premises in which the trafficker maintains his supply of narcotics, paraphernalia used in narcotics trafficking such as cutting and packaging materials, and other evidence of

illegal narcotics trafficking, including records and financial information. Similarly, knowledge of the location of the trafficker when he places telephone calls to known suppliers and customers can assist law enforcement in this physical surveillance of the subject and in obtaining further relevant evidence of the target's illegal narcotics trafficking activity. The use of a cellular telephone requires that the caller's signal involve the use of cell site in the service provider's system. When the target telephone is a cellular telephone, the location of this cell site and the direction from which the caller's signal was sent provides relevant information to assist law enforcement in the above functions.

11. Accordingly, it is requested that the [INSERT NAME OF SERVICE PROVIDER] listed in the accompanying proposed order, 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 be issued, disclose the location of cell site/sector (physical address) at call origination (for outgoing calls) call termination (for incoming calls), and if reasonably available, during the progress of a call, for the cellular telephone [INSERT CELLULAR TELEPHONE NUMBER].

12. It is further requested that the Court's order apply not only to [INSERT CELLULAR TELEPHONE NUMBER], but also [b7E]

[b7E]

b7E

b7E

b7E

b7E

] which are listed to

the same subscriber and wireless telephone account number as the subject cellular telephone number within the sixty (60) day period authorized by this order.

13. Because disclosure of this application could jeopardize the investigation for which the authorization to install and use the pen register, trap and trace and caller identification device is sought, the Applicant further requests that this application be filed under seal, pursuant to Title 18, United States Code, Section 3123(d)(1). The Applicant further requests that this Court's Order, and any subsequent Orders, be sealed until otherwise ordered by the Court.

WHEREFORE, it is respectfully requested that the Court grant an Order for a period of sixty (60) days, (1) authorizing the installation and use of a pen register to record numbers dialed or pulsed from [INSERT CELLULAR TELEPHONE NUMBER]; (2) authorizing the installation and use of a trap and trace and caller identification device to capture the incoming electronic or other impulses which identify the originating number of a wire or electronic communication to [INSERT CELLULAR TELEPHONE NUMBER]; (3) directing [INSERT SERVICE PROVIDER] to furnish forthwith to agents of the

[INSERT NAME OF AGENCY] all information, facilities, and technical assistance necessary to accomplish the installation and use of the devices unobtrusively and with minimum interference to the service presently accorded persons whose dialings or pulsings are the subject of the pen register, trap and trace, and caller identification device; and (4) directing [INSERT NAME OF SERVICE PROVIDER] and any other service provider of electronic communications services to provide agents of the [INSERT NAME OF AGENCY] with all subscriber names and addresses, telephone locations and dates of service, as well as all information regarding the means and source of payment for service, for all numbers dialed or pulsed from, or making incoming calls to [INSERT CELLULAR TELEPHONE NUMBER]; (5) to disclose the location of cell site/sector (physical address) at call origination (for outgoing calls), call termination (for incoming calls), and if reasonably available, during the progress of the call, for cellular telephone number [INSERT CELLULAR TELEPHONE NUMBER]; and (6) sealing this Application and the Court's Order.

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

EXECUTED on this _____ day of _____, 2004.

Respectfully submitted,

JEFFREY A. TAYLOR
UNITED STATES ATTORNEY
D.C. Bar No. 451-058

[INSERT NAME OF AUSA]
ASSISTANT UNITED STATES ATTORNEY
555 4th Street, NW
Washington, D.C. 20001
D.C. BAR NO. [AUSA'S BAR NUMBER]

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE)
APPLICATION OF THE UNITED)
STATES OF AMERICA FOR AN ORDER) MISC. NO. _____
AUTHORIZING THE INSTALLATION)
AND USE OF A PEN REGISTER, TRAP) UNDER SEAL
AND TRACE, AND CALLER)
IDENTIFICATION DEVICE ON CELLULAR)
TELEPHONE NUMBER [TELEPHONE NUMBER])
AND DISCLOSURE OF SUBSCRIBER)
INFORMATION)

ORDER

This matter having come before the Court pursuant to an application under Title 18, United States Code, Section 3122, by [INSERT NAME OF AUSA], an attorney for the Government, which application requests an Order under Title 18, United States Code, Section 3123, authorizing the installation and use of a pen register, trap and trace, a caller identification device, and cell site information on [INSERT CELLULAR TELEPHONE NUMBER], a cellular telephone, Electronic Serial Number (ESN) [INSERT ESN] and under Title 18, United States Code, Sections 2703(c)(1)(B) and 2703(d), directing the disclosure of subscriber records and information likely to be obtained by such installation and use, and that the disclosure of such records is relevant to an ongoing criminal investigation into possible violations committed by the user(s) of the cellular telephone and others of federal law, including [INSERT CODE CITATION], and

IT APPEARING that the numbers dialed or pulsed to and from the cellular telephone bearing [INSERT CELLULAR TELEPHONE NUMBER], a cellular telephone, Electronic Serial Number (ESN) [INSERT ESN] subscribed to by [INSERT NAME AND ADDRESS OF SUBSCRIBER], are relevant to an ongoing criminal investigation of possible violations of [INSERT CODE CITATIONS] and

IT FURTHER APPEARING that there are reasonable grounds to believe that the contents of the requested records, subscriber information and cell site information are relevant and material to an ongoing criminal investigation described in the application;

IT IS ORDERED, pursuant to Title 18, United States Code, Section 3123, that agents of the [INSERT NAME OF AGENCY] may install and use (1) a pen register to register numbers dialed to or pulsed from [INSERT CELLULAR TELEPHONE NUMBER], to record the date and time of such dialings or pulsings, and to record the length of time the telephone receivers in question are off the hook for incoming or outgoing calls; and (2) a trap and trace and caller identification device on [INSERT CELLULAR TELEPHONE NUMBER] to capture the incoming electronic and other impulses which identify the originating number of a wire or electronic communication and the date and time of such incoming pulses, for a period of sixty (60) days; and

IT IS FURTHER ORDERED that the information obtained from the caller identification feature provided pursuant to this Order shall

be [b7E]
[b7E]
[b7E] and

IT IS FURTHER ORDERED, pursuant to Title 18, United States Code, Section 3123(b)(2), that [INSERT NAME OF SERVICE PROVIDER] shall furnish agents of the [INSERT NAME OF AGENCY] forthwith all information, facilities, and technical assistance necessary to accomplish the installation of the devices unobtrusively and with minimum interference with the services that are accorded persons whose dialings and pulsings are the subject of the pen register, the trap and trace and the caller identification device; and

IT IS FURTHER ORDERED, that the [INSERT NAME OF SERVICE PROVIDER] provider shall be compensated by the applicant for reasonable expenses incurred in providing technical assistance; and

IT IS FURTHER ORDERED, pursuant to Title 18, United States Code, Sections 2703(c)(1)(B) and 2703(d), that, for each telephone number for which they possess such information, [INSERT NAME OF SERVICE PROVIDER] and any other provider of electronic communication service shall provide to agents of the [INSERT NAME OF AGENCY] all subscriber information, including subscriber name and address, telephone location, and length of service, as well as all information regarding the means and source of payment for service, for all telephone numbers dialed or pulsed from cellular telephone

number [INSERT CELLULAR TELEPHONE NUMBER], as indicated by the pen register, and all telephone numbers calling [INSERT CELLULAR TELEPHONE NUMBER], as indicated by the trap and trace and caller identification device, whether published or non-published, and

IT IS FURTHER ORDERED, pursuant to Title 18 U.S.C. §2703(d) that [INSERT NAME OF SERVICE PROVIDER] shall provide the cell site/sector (physical address) at call origination (for outgoing calls), call termination (for incoming calls), and it reasonably available, during the progress of the call, for cellular telephone number [INSERT CELLULAR TELEPHONE NUMBER], and

IT IS FURTHER ORDERED, that this Order shall apply not only to [INSERT CELLULAR TELEPHONE NUMBER], but also [b7E]

[b7E
b7E
b7E
b7E
b7E]

b7E] which are listed to the same subscriber and wireless telephone account number as the subject cellular telephone number within the sixty (60) day period authorized by this order.

IT IS FURTHER ORDERED, pursuant to Title 18, United States Code, Section 3123(d), that this Order and the application shall be sealed until otherwise ordered by the Court, and that [INSERT NAME

OF SERVICE PROVIDER], its agents, employees and affiliates, shall not disclose the existence of the pen register, trap and trace or caller identification device or the existence of the investigation to the listed subscriber, or to any other person, unless or until otherwise ordered by the Court.

SO ORDERED this _____ day of _____, 2004.

UNITED STATES MAGISTRATE JUDGE

[DATE]

**Court Order & Memorandum Opinion
of
United States District Court
Judge Thomas F. Hogan
Dated August 25, 2006
In case Number 06-0186, 187,& 188**

This document contains redactions made by the Court

These pages are not included in our page count

FILED

AUG 25 2006

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

CLERK, U.S. DISTRICT COURT
DISTRICT OF COLUMBIA

IN THE MATTER OF THE APPLICATION)
OF THE UNITED STATES OF AMERICA)
FOR AN ORDER AUTHORIZING THE)
MONITORING OF GEOLOCATION AND)
CELL SITE DATA FOR A SPRINT)
SPECTRUM CELL PHONE NUMBER)

Misc. No. 06-0186, 187, 188

UNDER SEAL

ESN [REDACTED])
CELL PHONE NUMBER [REDACTED])
ESN [REDACTED])
CELL PHONE NUMBER [REDACTED])
ESN [REDACTED])

ORDER

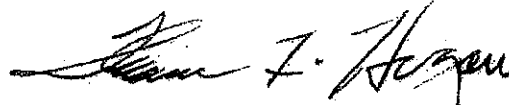
It is hereby

ORDERED that the Clerk of the Court is directed to not to seal the accompanying redacted Memorandum Opinion, dated May 25, 2006, and to make the redacted Memorandum Opinion available to the public. It is further

ORDERED that the unredacted original Memorandum Opinion in the above captioned case, dated May 25, 2006, shall remain **UNDER SEAL**.

SO ORDERED.

August 25th, 2006



Thomas F. Hogan
Chief Judge

FILED

AUG 25 2006

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

CLERK, U.S. DISTRICT COURT
DISTRICT OF COLUMBIA

IN THE MATTER OF THE APPLICATION)
 OF THE UNITED STATES OF AMERICA)
 FOR AN ORDER AUTHORIZING THE)
 MONITORING OF GEOLOCATION AND)
 CELL SITE DATA FOR A SPRINT)
 SPECTRUM CELL PHONE NUMBER)
 [REDACTED] ESN [REDACTED])
 CELL PHONE NUMBER [REDACTED])
 ESN [REDACTED])
 CELL PHONE NUMBER [REDACTED])
 ESN [REDACTED])

Misc. No. 06-0186, 187, 188

MEMORANDUM OPINION

Pending before the Court is the Government's Request for Cell Site and Geolocation Information. This matter comes to the Court as an appeal from the denial of this request by a Magistrate Judge.¹ Having carefully considered the Government's request, the arguments made at the hearing held on this issue, and the entire record herein, the Court will grant the application because the Government has made a showing of probable cause sufficient to obtain a warrant for the requested information.

I. BACKGROUND

A. Factual History

The application at issue seeks a Court Order authorizing the Government to monitor the geolocation and cell site information for three cellular telephones. Cell site data provides the

¹ The Government seeks review pursuant to Civil Rule 40.7(g) of the Rules of the United States District Court for the District of Columbia, which states that "the Chief Judge shall . . . hear and determine requests for review of rulings by magistrate judges in criminal cases not already assigned to a judge of the Court . . ."

location of the cell phone tower supplying service to a cell phone when it is actually engaged in a call. This provides a general location of where the phone is located at the time of the call. Cell site data can be obtained from the cell phone service provider with a delay of only a few seconds. Geolocation information can give the location of a cell phone within several hundred meters. This information cannot be provided in real time. The government can, however, obtain it by making a request to the service provider to get the specific location of the phone at a particular time.

The Government seeks this information because an ongoing investigation has established that members of a drug organization, [REDACTED] are presently in the Washington, D.C. area with a large quantity of drugs. [REDACTED] Aff. ¶ 11. [REDACTED]

[REDACTED] Two of the target cell phones are used by a customer of the organization [REDACTED], and the third is used by one of the members of the organization [REDACTED]: *Id.* ¶¶ 13, 14. Accordingly, the Government believes that tracking the locations of the cell phones will lead to the location of [REDACTED] the drugs. In [REDACTED] affidavit, Detective [REDACTED] affirms that there is probable cause to believe that the geolocation and cell site information for the target cell phones would provide evidence of activity in violation of 21 U.S.C. § 846, conspiracy to distribute and possess with intent to distribute controlled substances.

B. Procedural History

In the application to the Magistrate Judge, the Government sought authorization pursuant

to the All Writs Act, 28 U.S.C. § 1651(a); the Stored Electronic Communication Act ("SCA"), 18 U.S.C. § 2703(c); and Federal Rule of Criminal Procedure 41. On April 28, 2006, Magistrate Judge Robinson denied the Government's request, finding that none of the authorities cited by the Government authorized the disclosure sought. See DAR Or., April 28, 2006. Magistrate Judge Robinson denied the Government's request under the SCA, citing a prior decision of Magistrate Judge Facciola of this Court. See In the Matter of the Application of the United States of America for an Order Authorizing the Release of Prospective Cell Site Information, 407 F. Supp. 2d 134 (D.D.C. 2006) (Facciola, M.J.) ("Facciola Opinion"). Further, she found that the All Writs Act does not provide authority to approve the Government's request, and that the Government's reliance on Rule 41 was misplaced because the Government had not requested a search warrant. See DAR Or., April 28, 2006.

II. ANALYSIS

The issue presented by the instant application is under what authority (if any) the Court may order the disclosure of prospective cell site and geolocation information. The Government proposes three possible sources of authority: (1) the All Writs Act; (2) a combination of the SCA and the Pen Register Statute; and (3) Rule 41 of the Federal Rules of Criminal Procedure.

In the area of electronic surveillance law, there are four broad categories of surveillance, each with its own well-established standard for obtaining court ordered disclosure or monitoring. See Electronic Communications Privacy Act of 1986 ("ECPA"), Pub. L. No. 99-508, 100 Stat. 1848 (1986). Those categories (arranged from highest to lowest order of legal process) are: (1) wiretaps, which are authorized pursuant to 18 U.S.C. §§ 2510-2522, upon what could be called a

“probable cause plus” showing;² (2) tracking devices, which are authorized pursuant to 18 U.S.C. § 3117, upon a standard probable cause showing; (3) stored communications and subscriber records, which are authorized pursuant to the SCA upon a showing of specific and articulable facts showing that there are reasonable grounds to believe that the data sought is relevant and material to an ongoing criminal investigation; and (4) pen registers and trap and trace devices, which are authorized pursuant to 18 U.S.C. §§ 3121-3127 (“Pen Register Statute”), upon the Government’s certification that the data sought is relevant to an ongoing criminal investigation. See In re Application of the United States of America for Pen Register and Trap/Trace Device with Cell Site Location Authority, 396 F. Supp. 2d 747, 753 (S.D. Tex. 2005) (“Smith Opinion”).

One of the most hotly debated issues in this area of law is into which of the above categories cell site data properly falls.³ One thing that is clear, however, is that Congress has expressly prohibited the use of pen registers and trap and trace devices to disclose the location of the person using the phone upon a mere certification that the information is relevant to an

² An application to intercept the contents of communications parallels a traditional warrant application: it must establish probable cause to believe that particularly described evidence of a specific crime will be found. In addition, Title III requires a showing that “normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous.” See 18 U.S.C. § 2518(3)(c). This additional requirement that a wiretap be used only as an investigative technique of last resort makes the Title III standard a “probable cause plus” showing.

³ Courts may order disclosure of *historical* cell site data pursuant to § 2703(c), as this type of data has been found to qualify as “information pertaining to a subscriber.” See 18 U.S.C. § 2703(c); In the Matter of the Application of the United States of America for an Order Authorizing the Installation and Use of a Pen Register and/or Trap and Trace for Mobile Identification Number (585) 111-1111 and the Disclosure of Subscriber and Activity Information under 18 U.S.C. § 2703, 415 F. Supp. 2d 211, 214 (W.D.N.Y. 2006) (Feldman, M.J.) (“Feldman Opinion”). In doing so, courts would use the “specific and articulable facts” standard. Here, the Government seeks disclosure of cell site information on a *prospective* basis.

ongoing investigation. See 47 U.S.C. § 1002(a)(2)(B) (“with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices . . . , such call identifying information shall not include any information that may disclose the physical location of the subscriber . . .”).⁴ Congress’ use of the word “solely” has given birth to the dominant theory put forward by the Government in the recent prospective cell site data cases, which has caused a split among the courts that have addressed the issue. That theory has become known as the “hybrid theory.”

The “hybrid theory” posits that the Court is authorized to order the disclosure of prospective cell site data under a combination of the SCA and the Pen Register Statute. The government argues that the use of the word “solely” necessarily implies that another authority

⁴ Support for the proposition that cell site and geolocation information may be obtained pursuant to Rule 41 can be found in the legislative history of the “solely” exception in the Patriot Act, codified as 47 U.S.C. § 1002(a)(2)(B), that gave birth to the “hybrid theory.” In order to alleviate the legislation drafters’ concern that the Government would be able to use information obtained from a pen register or trap and trace device to track a person upon a mere certification that data sought is relevant to an ongoing criminal investigation, then FBI Director Louis Freeh stated:

Some cellular carriers do acquire information relating to the general location of a cellular telephone However, this information is not the specific type of information obtained from “true” tracking devices, which can require a warrant or court order Even when such generalized location information . . . is obtained from communications service providers, court orders or subpoenas are required and obtained.

Statement of Louis J. Freeh, Director, FBI, Before the Senate Joint Judiciary Technology, Law, Civil and Constitutional Rights Subcommittees at 29 (March 18, 1994) reprinted in Federal Document Clearing House, 1994 WL 223962. Director Freeh’s statement appears to contemplate that physical location information would be available to the Government through obtaining a warrant.

may be combined with the Pen Register Statute to authorize disclosure. See Gov. App. at 6 n.7. Most of the Magistrate Judges that have considered the hybrid theory have found it to be unavailing, holding that the Pen Register Statute and the SCA in tandem do not provide authority for disclosure of prospective cell site data. See, e.g., In re Application of the United States of America for an Order Authorizing the Use of a Pen Register and a Trap and Trace Device, 396 F. Supp. 2d 294, 318-321 (E.D.N.Y. 2005) ("Orenstein Opinion"); Smith Opinion, 396 F. Supp. 2d at 761-765. The first District Court to rule on the hybrid theory, however, has come out the other way, finding that this combination does allow for disclosure. See In the Matter of the Application of the United States of America for an Order: Authorizing the Installation and Use of a Pen Register and Trap and Trace Device, and (2) Authorizing Release of Subscriber and Other Information, Misc. No. H-06-0085 (S.D. Tex. April 11, 2006) (Rosenthal, J.); see also In the Matter of the United States for an Order: (1) Authorizing the Installation and Use of a Pen Register and Trap and Trace Device; and (2) Authorizing Release of Subscriber Information and/or Cell Site Information, 411 F. Supp. 2d 678, 682-83 (W.D. La. 2006) (Hornsby, M.J.); In re Application of the United States of America for an Order for Disclosure of Telecommunications Records and Authorizing the Use of a Pen Register and Trap and Trace, 405 F. Supp. 2d 435, 448-49 (S.D.N.Y. 2005) (Gorenstein, M.J.).

The Court does not reach the question today of whether the Pen Register Statute and SCA in combination provides authority for the Court to order disclosure. That is because, for the reasons set forth below, the Court agrees with what is thus far the majority view that prospective cell site and geolocation information is available upon a traditional probable cause showing under Rule 41. As the Government has indeed made such a showing, the Court need not decide

whether the much-debated "hybrid" approach would provide an alternative source of authority.

Under Rule 41, a warrant may issue for "(1) evidence of a crime; (2) contraband, fruits of crime, or other items illegally possessed; (3) property designed for use, intended for use, or used in committing a crime; or (4) a person to be arrested or a person who is unlawfully restrained," upon a probable cause showing. Fed. R. Crim. P. 41. Here, the government has submitted an application to a judicial officer authorized to issue warrants under Rule 41(b), that seeks permission to seize information that the applicant states is evidence of a crime.

Among the Courts that have denied prospective cell site applications based upon the hybrid theory, all that have considered the applicability of Rule 41 have concluded that prospective cell site data would be available upon a probable cause showing. See In the Matter of the Application of the United States of America for Orders Authorizing the Installation and Use of Pen Registers and Caller Identification Devices on Telephone Numbers [SEALED] and [SEALED], 416 F. Supp. 2d 390, 390 (D. Md. 2006) (Bredar, M.J.) ("the court may only authorize disclosure of prospective cell site information upon a showing of probable cause pursuant to Rule 41"); Feldman Opinion, 415 F. Supp. 2d at 219 ("The Court will, however, issue a warrant for the seizure of the requested real time cell location information upon a showing that there exists probable cause to believe that the data sought will yield evidence of a crime,"); Facciola Opinion, 407 F. Supp. 2d at 135 ("If one accepts, as I do, that . . . the information the government seeks can only be secured by a warrant issued pursuant to Rule 41 of the Federal Rules of Criminal Procedure, the standard that pertains to the issuance is, as the Fourth Amendment requires, probable cause to believe that the information sought is itself evidence of a crime . . ."); In the Matter of the Application of the United States of America for

an Order Authorizing the Installation and Use of a Pen Register and a Caller Identification System on Telephone Numbers [SEALED] and [SEALED] and the Production of Real Time Cell Site Information, 402 F. Supp. 2d 597, 605 (D. Md. 2005) (“When the government seeks to acquire and use real time cell site information to identify the location and movement of a phone and its possessor in real time, the court will issue a warrant upon a sworn affidavit demonstrating probable cause to believe the information will yield evidence of a crime.”); Orenstein Opinion, 396 F. Supp. 2d at 321 (“to the extent that the government seeks a judicial imprimatur for its acquisition in real time of prospective cell site information, it must proceed under Rule 41”); Smith Opinion, 396 F. Supp. 2d at 765 (“Denial of the Government’s request for prospective cell site data in this instance should have no dire consequences for law enforcement. This type of surveillance is unquestionably available upon a traditional probable cause showing under Rule 41.”); [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

This Court agrees with the majority rule that Rule 41 governs the application here.⁶

⁵ [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

⁶ In his first opinion on the issue, Magistrate Judge Facciola of this Court expressed concern, without deciding, that a person’s location in itself may not meet any of the criteria set forth in Rule 41. See In the Matter of the Application of the United States of America for an Order Authorizing the Release of Prospective Cell Site Information, 407 F. Supp. 2d 132, 133 (D.D.C. 2005) (Facciola, M.J.). The Court finds that the location of a cell phone, and thus the

What the government is effectively seeking in its application, is to convert the targeted cell phones into tracking devices. See Orenstein Opinion, 396 F. Supp. 2d at 321. "The use of [tracking devices] in the detection of crime is a valuable and well-accepted law enforcement tool." In re Application of United States for an Order Authorizing the Installation, Monitoring, Maintaining, Repairing, and Removing of Electronic Transmitting Devices ("Beepers") and Infrared Tracking Devices on or Within a White Ford Truck VIN 1FDKE37H3HHB79229, 155 F.R.D. 401, 402 (D. Mass. 1994) ("White Truck"). Tracking devices, in the rubric of electronic surveillance erected by Congress in the ECPA, are governed by Rule 41. See 18 U.S.C. § 2703(c); White Truck, 155 F.R.D. at 403. Here, the Government has made a showing of probable cause to believe that the geolocation and cell site information for the target cell phones would provide evidence of activity in violation of 21 U.S.C. § 846, conspiracy to distribute and possess with intent to distribute controlled substances. Accordingly, the Court will issue a warrant.

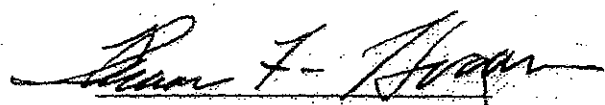
III. CONCLUSION

For the aforementioned reasons, the Court finds that prospective cell site and geolocation information is available upon a traditional probable cause showing under Rule 41 of the Federal Rules of Criminal Procedure, and that the Government has indeed made such a showing.

suspect's location, may qualify as "evidence of a crime." In United States v. Karo, the Supreme Court held that the Government must obtain a warrant before monitoring tracking devices that are transmitting from inside private premises, 468 U.S. 705, 717-18 (1984). Implicit in that decision is the recognition that tracking devices provide information that is subject to search or seizure under Rule 41. See id. Cell site and geolocation information may be evidence of a crime because, for example, a subject's location can be used to rebut an alibi or place him at the scene of a crime. See Facciola Opinion, 407 F. Supp. 2d at 135. Here, the location of a suspect known to be purchasing narcotics, or of one known to be guarding and selling a large quantity of narcotics, is likely to reveal the location of the drug stash house.

Accordingly, the Court has granted the application and issued a warrant pursuant to Rule 41 to obtain the cell site and geolocation information sought. The Order granting the Government's application was issued by the Court on May 4, 2006.

May 25th, 2006


Thomas F. Hogan
Chief Judge