



U.S. Department of Justice

Criminal Division

Office of Enforcement Operations

Washington, D.C. 20530

August 29, 2018

Via E-Mail

Linda Lye, Esq.
American Civil Liberties Union Foundation of
Northern California
39 Drumm Street
San Francisco, CA 94111
llye@aclunc.org

ACLU-NC v. DOJ, N.D. Cal. Case No. 3:12-
cv-04008-MEJ

Dear Ms. Lye:

Please find attached the relevant sections of USABook, which have been re-processed in accordance with the Ninth Circuit's guidance in *ACLU of Northern California v. U.S. Dep't of Justice*, 880 F.3d 473 (9th Cir. 2018). Feel free to contact Brad Rosenberg or me if you have any questions about this disclosure.

Sincerely,

A handwritten signature in black ink, appearing to read "Peter C. Sprung".

Peter C. Sprung
Trial Attorney
FOIA/PA Unit
(202) 305-4042

Enclosures

cc: Brad Rosenberg, Esq. (w/encls.)

Withheld in Full: 105 pages (b)(5) AWP, ACP

+
L7E

CRM
4

USABook > Electronic Surveillance > Tracking Devices Manual > **Preface**

Preface

This manual provides guidance on the use of a variety of methods for locating or tracking persons and property. Increasingly frequent inquiries in recent years from federal prosecutors and agents about these techniques—as well as sharply conflicting case law in at least one area—underscore the need for clear and comprehensive written advice.

Each chapter of the manual addresses a specific method or technology, beginning with a technical overview. The majority of each chapter discusses the relevant statutory and constitutional provisions, analyzes pertinent judicial precedent, and provides concrete recommendations on specific points of practice and procedure. Where appropriate, the discussion notes adverse decisions and potential objections—whether at the initial application stage or on a motion to suppress—and suggests legal strategies for responding to each. Recommended form pleadings appear in the Appendix.

Extremely valuable criticisms and suggestions on early drafts of this manual came from Collin Bruce, Patrick Caruso, Steve Heymann, (b) (6), (b) (7)(C), John Horn, (b) (6), (b) (7)(C), Seth Kosto, (b) (6), (b) (7)(C), (b) (6), (b) (7)(C), (b) (6), (b) (7)(C), (b) (6), (b) (7)(C), Janet Webb, and Julie Wuslich. (b) (6), (b) (7)(C) at the Office of Legal Education provided prompt and capable assistance in preparing the documents for USABook. The author is deeply grateful for all of their contributions.

Questions, comments, or suggestions about the manual may be directed to the author at Mark.Eckenwiler@usdoj.gov or (b) (6), (b) (7)(C).

The manual serves only as internal Department of Justice guidance. It is not intended to, does not, and may not be relied upon to create any rights, substantive or procedural, enforceable at law by any party in any matter civil or criminal.

August 2009

USABook > Electronic Surveillance > Tracking Devices Manual > **Roadmap/FAQs**

Roadmap/FAQs

Is cell-site information the same as GPS location information?

No. See Part I.A.

What kind of legal process do I need in order to locate a cell phone?

A summary:

	Prospective Information	Historical Information
E-911/Geolocation	Rule 41 warrant	n/a
Cell-Site (and Satellite Phone) Records	Pen register/trap and trace order, in conjunction with 18 U.S.C. § 2703(d) court order ("hybrid order")	18 U.S.C. § 2703 (d) court order

For detailed information, see Part I.B (including the discussion of emergency authorities in I.B.5).

What does it mean to "ping" a phone?

The term has no fixed meaning, and should be avoided to prevent confusion. See Part I.A.2.

How precise is the phone location information available from a service provider?

E-911/geolocation information (including but not limited to GPS) can be precise to 50 meters or less. Cell-site location information precision varies from a few hundred meters in urban centers to 20 miles or more in rural areas. See Part I.A.

Does cell-site information implicate a Fourth Amendment interest?

No. A few courts have insisted that it does, but that conclusion is based on a fundamental misunderstanding of the technology. See Part I.B.3.b.

Is a target's cell phone a "tracking device" under 18 U.S.C. § 3117?

No. See Part I.B.3.b.

Do I need a court order to install and use a tracking device on a vehicle?

Possibly, depending on where (and how) the installation is to be performed and on the characteristics of the device. See Part II.C.

Is OnStar a "tracking device" under 18 U.S.C. § 3117?

No. See Part III.B.

How can I obtain additional help with go-bys, legal briefing, or general questions?

Contact OEO Associate Director Mark Eckenwiler at (b) (6), (b) (7)(C) or mark.eckenwiler@usdoj.gov.

USABook > Electronic Surveillance > Tracking Devices Manual > **Part I.**
next | help

Part I.

Obtaining Location Information from Wireless Carriers

- A. Technology Basics
 - 1. Cell-Site Information: Towers and Sectors
 - 2. E-911"/Geolocation Information
 - 3. Satellite Phones
- B. Legal Authority Necessary to Obtain Location Information
 - 1. Compelled Disclosure of Prospective E-911/Geolocation Information
 - 2. Compelled Disclosure of Historical E-911/Geolocation Information
 - 3. Compelled Disclosure of Prospective Cell-Site (or Satellite Phone) Information
 - a. Procedural issues
 - b. Substantive objections (and responsive arguments)
 - c. Table of decisions analyzing "hybrid theory" (by circuit and district)
 - 4. Compelled Disclosure of Historical Cell-Site (or Satellite Phone) Location Information
 - a. Procedural issues
 - b. Substantive objections (and responsive arguments)
 - 5. Emergency Disclosures
 - a. Voluntary disclosure
 - b. Compelled disclosure
- C. Responding to Suppression Motions
 - 1. No Statutory Suppression Remedy Exists
 - 2. Fourth Amendment Suppression Inapplicable
 - a. Voluntary disclosure to third party (business records)
 - b. No "search" occurs where location information does not reveal facts about the interior of a private location
 - c. Lack of standing with respect to another person's phone
 - d. Arrest warrant authorizes ancillary searches
- D. Comprehensive List of Federal Cases (as of August 2009)

A. Technology Basics

1. Cell-Site Information: Towers and Sectors

Cellular telephone networks provide service to their customers through antennas deployed across the provider's coverage area. When the user places an outbound call, the handset transmits that communication over the airwaves to a nearby tower antenna, which relays the call to a local switch for routing. Conversely, whenever another party places a call to a user's cellular telephone, the network "pages" that phone to alert the owner to the incoming call; if the owner answers, the call is put through and (as before) carried by a tower near the phone. In either scenario, a phone may move in the course of a single call through the coverage areas of multiple towers, especially where the user is in a moving vehicle. In most instances, the network enables seamless "handoffs" from one tower to the next without the user's knowledge. As a result, the system's awareness of a wireless phone's general whereabouts is essential to providing cellular service.

Spacing between antenna towers varies enormously depending on a number of factors, especially terrain and population density. In a heavily populated area such as lower Manhattan, towers may be spaced every few hundred yards; in rural areas, by contrast, towers may be separated by 20 miles or more; and towers in suburban or small urban areas will typically be spaced in a range between those extremes.

Except in sparsely populated areas, a typical tower will have three separate antenna **faces** (also called **sectors**), with each face serving a 120-degree portion of the roughly circular coverage area extending out from the antenna mast. For many carriers, the three sectors can be visualized as the areas on a clock face from 10 to 2; from 2 to 6; and from 6 to 10. In rural coverage areas, a tower may simply have a single 360-degree face.

Whenever a cellular phone user initiates or receives a communication—such as a voice call or text message—the carrier routinely creates a record, including the date and exact time, of the tower and sector handling the communication at the start and end of the communication.[FN1] Service providers typically retain these routine business records for several months or longer.

In addition to these historical records, carriers have certain legal obligations with respect to prospective—that is, real-time—location information sought by law enforcement. Specifically, the FCC requires carriers to be technically capable of delivering real-time cell-site data at the start and end of calls.[FN2]

Whether obtained prospectively or from historical records, cell-site records cannot reveal a phone's exact location. As noted above, even in heavily populated urban centers a tower's service radius is several hundred yards. Moreover, because of variable factors such as terrain and network congestion, the tower serving a particular communication is not necessarily the tower closest to the phone.[FN3]

As discussed in section B.3.b below, several courts have erroneously asserted that cell-site location information is much more precise. In general, these courts have confused cell-site records with the entirely distinct type of location information discussed in the next section.

2. "E-911"/Geolocation Information

When a landline subscriber places an emergency call to 911, the service address of the phone is automatically transmitted to the 911 call center. In the early years of cellular service, however, no equivalent capability existed for wireless callers. As a result of this gap, first responders were often unable to locate kidnapping victims, lost/injured/disoriented individuals, and other emergency callers.

Recognizing the problem, in 1996 the FCC began requiring wireless carriers to develop and implement systems by 1998 to automatically deliver wireless location information during emergency calls. For this initial phase—E-911 Phase I b carriers were required only to deliver cell-site information.[FN4] However, it rapidly became apparent that the limited accuracy of cell-site data was inadequate to meet the needs of emergency responders attempting to locate a distressed caller.

Accordingly, in 2003 the FCC promulgated "E-911 Phase II" regulations imposing more stringent location precision requirements.[FN5] Carriers were allowed to choose from a variety of available technologies; some opted to use Global Positioning System (GPS) technology in new customer handsets, while others opted for "multilateration" methods (often referred to informally as "triangulation") relying on signal measurements made from multiple towers.[FN6] Unlike cell-site information, which provides only the location of the physical network infrastructure (cell tower) in the vicinity of a phone, E-911 Phase II information indicates the location of the phone itself.

Depending on the type of technology selected, the FCC regulations generally require E-911 location information to be precise to within 50-300 meters. Strict compliance with the regulations has been uneven, with several carriers fined for failure to meet the standards. However, E-911 Phase II information may at times exceed the FCC requirements and provide location information precise to under 50 meters.[FN7]

In most circumstances, a wireless carrier may take advantage of these same capabilities at the request of law enforcement even when no 911 call is made. Agents frequently refer to this

process as "**pinging**" a phone; **because this slang term is ambiguous** (sometimes referring instead to obtaining cell-site data), **OEO strongly recommends against its use, especially in court filings.**

3. Satellite Phones

Because satellite phone networks, such as Iridium, do not rely on terrestrial antenna towers, cell-site information *per se* does not exist. Depending on a number of factors, however, satellite phone providers may be able to provide both historical and prospective location information roughly comparable in precision to cell-site records.

B. Legal Authority Necessary to Obtain Location Information

The types of location information described above may be obtainable either through legal process—that is, compelled disclosure—or through voluntary disclosure by the provider.

The following chart summarizes OEO's recommendations for how to compel a service provider to disclose wireless location information:

	Prospective Information	Historical Information
E-911/Geolocation	Rule 41 warrant	n/a
Cell-Site (and Satellite Phone) Records	Pen register/trap and trace order, in conjunction with 18 U.S.C. § 2703(d) court order ("hybrid order")*	18 U.S.C. § 2703 (d) court order

* In a situation involving immediate danger of death or serious bodily injury, rely upon the emergency provision of the pen register/trap and trace statute (18 U.S.C. § 3125) and make a followup "hybrid" application to the court within 48 hours. Note that section 3125 requires Department approval (coordinated through OEO) prior to emergency use or installation of a pen register/trap and trace device. (See section B.5 below for further details.)

Separately, a service provider may voluntarily disclose historical location information in a situation involving immediate danger of death or serious bodily injury, pursuant to 18 U.S.C. § 2702(c)(4). Note that where disclosure is made voluntarily, followup compulsory process is both unnecessary and inadvisable.

For a detailed analysis of each of these authorities, including emergency access to location information, see the following sections.

1. Compelled Disclosure of Prospective E-911/Geolocation Information

For several reasons, including the information's potentially high degree of precision, OEO recommends that demands for ongoing E-911/geolocation information be made pursuant to a warrant issued under Federal Rule of Criminal Procedure 41. (See the model forms in the Appendix.) A number of courts have expressly endorsed the practice of relying on Rule 41.[FN8]

This approach raises a number of procedural issues, including

- **applicability of Rule 41's "tracking device" provisions:** As discussed in section B.3.b below, OEO believes (and several courts have held) that "tracking device" means only a

device physically installed by the government without the knowledge of the tracked property's owner. As discussed below, treating a target's phone as a "tracking device" conflicts with the text and history of the tracking device statute (18 U.S.C. § 3117) and creates problems in related areas such as Title III.

Accordingly, we recommend against invoking or relying upon 18 U.S.C. § 3117 or the corresponding "tracking device" provisions in Rule 41 (added in 2006) when seeking location information about a target's phone. For the same reasons, we advise against using AO Forms 102 through 104 (search warrant for "tracking device").

Notwithstanding the lack of provisions in Rule 41 (apart from the tracking device language), we are confident that a warrant issued under the Rule may be used for prospective surveillance. Courts have long found Rule 41 an appropriate means of authorizing other types of ongoing surveillance—surreptitious video surveillance[FN9] and pen registers[FN10]—not expressly mentioned in the text of the Rule.

- which district to apply in: Rule 41(b)(2) states that a warrant may issue for "a person or property outside the district if [it] is located within the district when the warrant is issued." However, the Criminal Division believes that 18 U.S.C. § 2703(c)(1)(A), which permits the compulsion of records and other information from service providers outside the district, overrides the limitations in Rule 41. Under this approach, prosecutors may obtain a warrant for prospective geolocation information from a "court of competent jurisdiction" (as defined at 18 U.S.C. § 2711(3)), including a court with jurisdiction over the offense under investigation, without regard to the location of the target phone.
- duration: We recommend seeking authorization for a maximum period of 30 days.
- describing the requested information: As discussed in section A.2 above, wireless carriers use different technologies to geolocate customer handsets: some use GPS technology, while others employ multilateration techniques (informally known as "triangulation"). Instead of referring to specific technologies, an application and order should use technology-neutral terms such as "geolocation information" or "latitude and longitude." The slang term "ping" (or "pinging") should be avoided.
- the form of the return: OEO recommends that the return inform the court of a) the date and time location monitoring began and b) the period during which it was obtained. Where a subsidiary request is made within a Title III wiretap order, OEO recommends that the court sign a separate warrant (see Appendix) to facilitate making the return.
- notice (and delaying it): Obviously, notice need not be given to the target during the period of location monitoring. Once the period has run, however, Rule 41 requires giving notice to the user of the target phone. Notably, Rule 41(f)(3) and 18 U.S.C. § 3103a(b) permit notice to be delayed for 30 days initially, plus extensions of 90 days each. These are the default periods; the statute allows for flexibility where circumstances justify it. (For instance, we believe that a request made in conjunction with a Title III application may permissibly seek to synchronize the Rule 41 notice, and thus the delay, with the timing of the Title III service of inventory.)

Prosecutors and agents in the Ninth Circuit should be aware of *United States v. Freitas*, [FN11] which holds that absent unusual circumstances, the Fourth Amendment forbids a delay of more than 7 days (subject to extension upon application to the court) in notifying the owner of premises searched pursuant to a delayed-notice warrant. This holding has been expressly rejected elsewhere,[FN12] and is manifestly incompatible with the provision in Title III permitting delay of notice of an interception order for up to 90 days.[FN13]

- whom to notify: We recommend giving notice to the person(s) known to have used the

target phone during the relevant period, and not merely to the registered owner, if different.

2. Compelled Disclosure of Historical E-911/Geolocation Information

Phone companies may maintain records reflecting the precise location data derived from E-911 sources. For guidance on compelled disclosure of these records, please contact OEO at (202) 353-5265, or CCIPS at (202) 514-1026.

3. Compelled Disclosure of Prospective Cell-Site (or Satellite Phone) Information

Because cell-site information constitutes "signaling information" within the meaning of the pen/trap statute,[FN15] a standard pen/trap order would normally suffice to compel a wireless carrier to deliver real-time cell-site information. However, in 1994 Congress enacted 47 U.S.C. § 1002(a)(2), which prohibits a carrier from disclosing "solely pursuant" to pen/trap authority "information that may disclose the physical location of the subscriber". In doing so, Congress did not explicitly declare what additional authority is required.

This omission has resulted in extensive litigation, producing at least 35 separate opinions from district court judges and magistrate judges, on which form of compulsory process is required of (or available to) law enforcement seeking prospective cell-site information. (See the table of cases in section B.3.c below.)

The Department believes that prospective cell-site information may be obtained using a court order issued under the combined authority of the pen/trap statute and 18 U.S.C. § 2703(d), requiring a showing of "specific and articulable facts." (A sample form is included in the Appendix.) At least four different district court judges[FN16] and three magistrate judges[FN17] have issued written opinions endorsing this approach, which has come to be known as the "hybrid theory." [FN18]

a. Procedural issues

Prosecutors seeking so-called hybrid orders for prospective cell-site information should be mindful of several procedural issues, including

- required showing: A hybrid application should not merely certify that the requested location information is relevant to an ongoing criminal investigation (as required under the pen/trap statute). Rather, the application should set forth specific facts in conformity with the section 2703(d) standard, and the order should make a specific finding that the application sets forth such facts.
- requested information: Prosecutors **should not** use the hybrid theory to request prospective "GPS data," "E-911 information," "tower triangulation records," "location information derived from multiple towers simultaneously," or similar formulations. (The same is true for ill-defined terms—*e.g.*, "pinging"—subject to misinterpretation.) However, satellite phone location information—which is roughly comparable in precision to cell-site information and is unrelated to GPS data—may properly be sought under the hybrid theory.
- duration: Hybrid orders may be obtained for a period of up to 60 days, as provided for under the pen/trap statute.

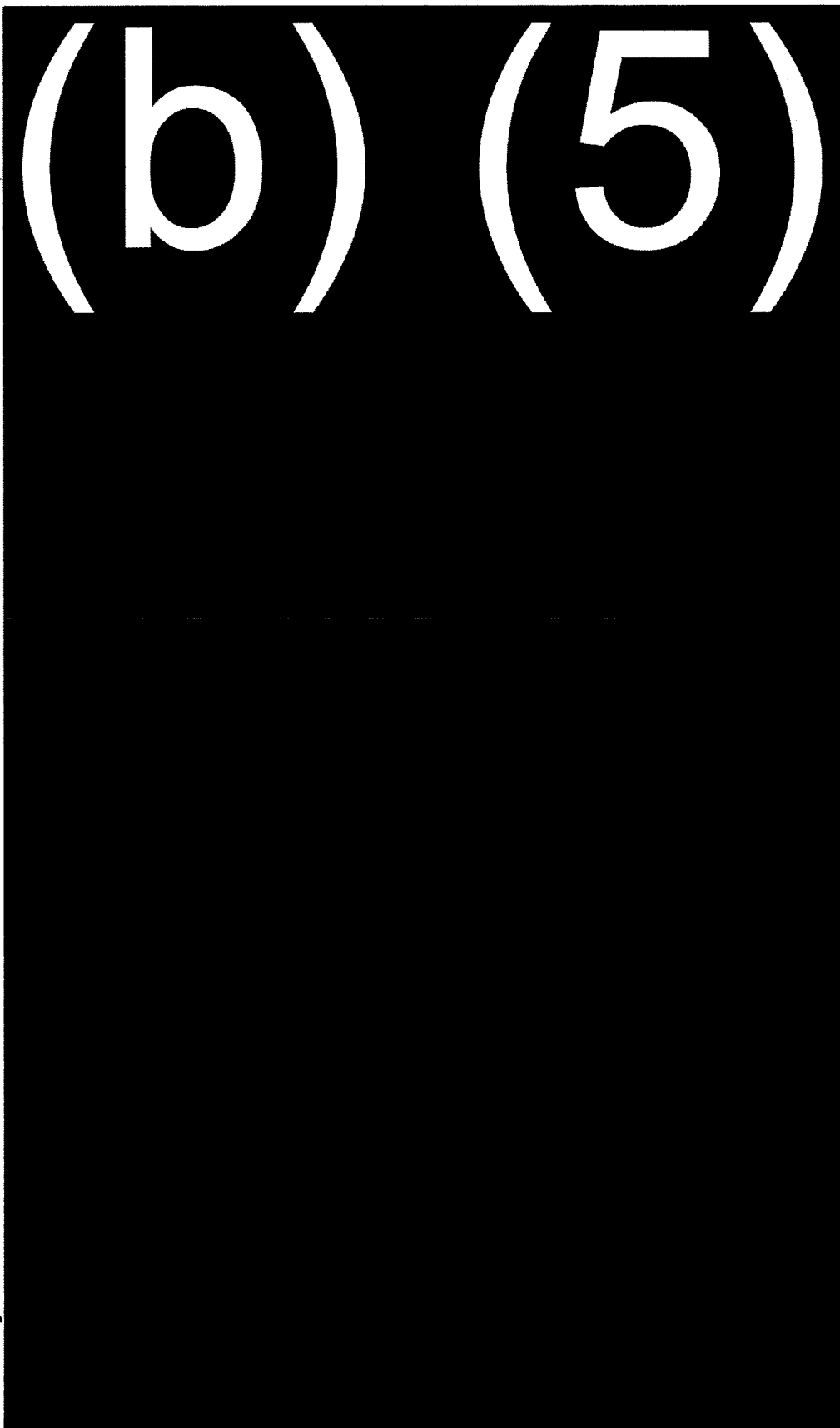
b. Substantive objections (and responsive arguments)

Judicial opinions rejecting the hybrid theory rely on a wide variety of rationales. This section addresses the most commonly recurring objections.

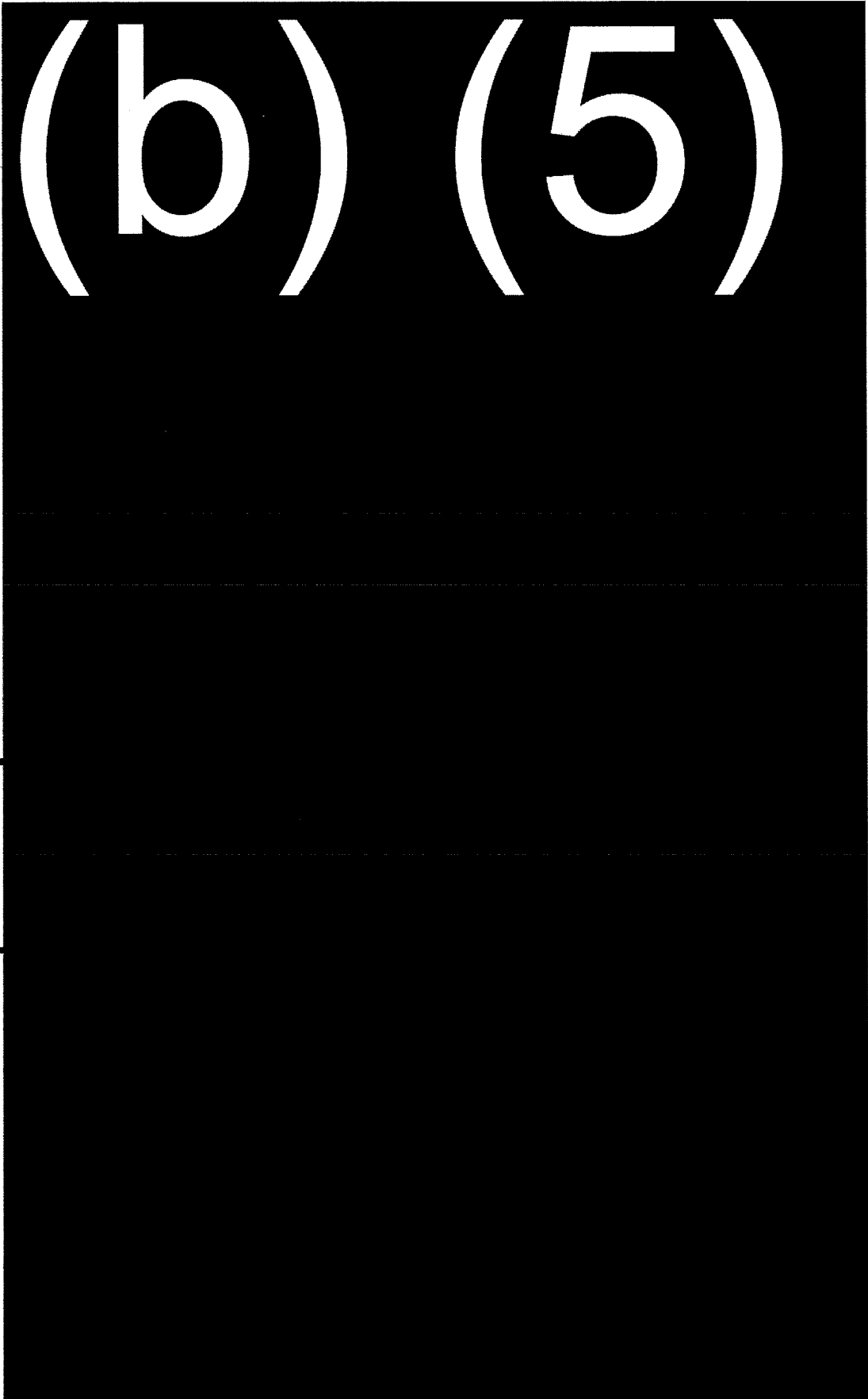
- "cell-site information is pinpoint accurate": Several courts have erroneously

referred to cell-site data as involving "triangulation," GPS, or E-911 Phase II capabilities,[FN19] in some cases claiming that the resulting information is extraordinarily precise.[FN20] As explained in Section A above, cell-site information is entirely distinct from—and appreciably less precise than—information obtained through those other location-finding techniques.

(b) (5)



(b) (5)



(b) (5)

c. Table of decisions analyzing "hybrid theory" (by circuit and district)

Case Citation	Accepts Hybrid Theory?	Level
1st Circuit		
<i>Alexander II Op.</i> , 530 F.Supp.2d 367 (D. Mass. 2007)	No, demands probable cause	Magistrate Judge
<i>McGiverin Op.</i> , 497 F.Supp.2d 301 (D.P.R. 2007)	No, demands probable cause	Magistrate Judge
2d Circuit		
<i>McMahon Op.</i> , 2009 WL 159187 (S.D.N.Y. Jan. 13, 2009)	No, demands probable cause	District Court
<i>Kaplan Op.</i> , 460 F.Supp.2d 448 (S.D.N.Y. 2006)	Yes	District Court
<i>Peck Op.</i> , 2006 WL 468300 (S.D.N.Y. Feb. 28, 2006)	No, demands probable cause	Magistrate Judge
<i>Gorenstein Op.</i> , 405 F.Supp.2d 435 (S.D.N.Y. 2005)	Yes	Magistrate Judge
<i>Cogan Op.</i> , No. M-08- 533 (E.D.N.Y. Jan. 12, 2009) (unpublished)	Yes	District Court
<i>Garaufis II Op.</i> , 2009 WL 1594003 (E.D.N.Y. Feb. 26, 2009)	Yes	District Court
<i>Pollak Op.</i> , 2009 WL 1530195 (E.D.N.Y. Feb. 12, 2009)	No, demands probable cause	Magistrate Judge (<i>rev'd, Garaufis II</i>)
<i>Garaufis I Op.</i> , 2008 WL 5082506 (E.D.N.Y. Nov. 26, 2008)	Yes	District Court
<i>Orenstein Op.</i> , 396 F.Supp.2d 294 (E.D.N.Y. 2005)	No, demands probable cause	Magistrate Judge
<i>Feldman Op.</i> , 415 F.Supp.2d 211 (W.D.N.Y. 2006)	No, demands probable cause	Magistrate Judge
3d Circuit		
<i>Lenihan Opinion</i> , 534 F.Supp.2d 585 (W.D. Pa. 2008); appeal pending	No, demands probable cause (in dicta)	Magistrate Judge
4th Circuit		
<i>Bredar III Op.</i> , 439 F.Supp.2d 456	No, demands	Magistrate Judge

CRM-0014

(D. Md. 2006)	probable cause	
<i>Bredar II Op.</i> , 416 F.Supp.2d 390 (D. Md. 2006)	No, demands probable cause	Magistrate Judge
<i>Bredar I Op.</i> , 402 F.Supp.2d 597 (D. Md. 2005)	No, demands probable cause	Magistrate Judge
<i>Stanley Op.</i> , 415 F.Supp.2d 663 (S.D. W. Va. 2006)	No (in dicta)	Magistrate Judge
5th Circuit		
<i>Rosenthal II Op.</i> , 2007 WL 3036849 (S.D. Tex. Oct. 17, 2007)	Yes	District Court
<i>Rosenthal I Op.</i> , 433 F.Supp.2d 804 (S.D. Tex. 2006)	Yes	District Court
<i>Owsley III Op.</i> , 2007 WL3355602 (S.D. Tex. Nov. 8, 2007)	Yes (in dicta)	Magistrate Judge
<i>Owsley II Op.</i> , 2007 WL 3342243 (S.D. Tex. Nov. 7, 2007)	Yes (in dicta)	Magistrate Judge
<i>Owsley I Op.</i> , 2007 WL 3341736 (S.D. Tex. Nov. 7, 2007)	Yes (in dicta)	Magistrate Judge
<i>Smith II Op.</i> , 441 F.Supp.2d 816 (S.D. Tex. 2006)	No, demands probable cause	Magistrate Judge
<i>Smith I Op.</i> , 396 F.Supp.2d 747 (S.D. Tex. 2005)	No, demands probable cause	Magistrate Judge
<i>Hornsby Op.</i> , 411 F.Supp.2d 678 (W.D. La. 2006)	Yes	Magistrate Judge
6th Circuit		
<i>Weir Op.</i> , No. 6:08-6038M- REW (E.D. Ky. Apr. 17, 2009) (unpublished)	No, demands probable cause	Magistrate Judge
7th Circuit		
<i>Lee Op.</i> , 2006 WL 1876847 (N.D. Ind. July 5, 2006)	No, demands probable cause	District Court
<i>United States v. Amaral- Estrada</i> , 2006 WL 3197181 (S.D. Ind. June 30, 2006)	No, demands probable cause	District Court (<i>aff'd on other grounds</i>)
<i>Adelman Op.</i> , 2006 WL 2871743 (E.D. Wis. Oct. 6, 2006)	No, demands probable cause	District Court (<i>aff'g Callahan Op.</i>)
<i>Callahan Op.</i> , 412 F.Supp.2d 947 (E.D. Wis. 2006)	No, demands probable cause	Magistrate Judge (<i>aff'd by Adelman</i>)
9th Circuit		
<i>Hollows II Op.</i> , 2007 WL 397129 (E.D. Cal. Feb. 1, 2007)	Yes	Magistrate Judge

<i>Hollows I Op.</i> , No. S-06-SW- 0041 (E.D. Cal. Mar. 15, 2006) (unpublished)	Yes	Magistrate Judge
11th Circuit		
<i>Presnell Op.</i> , No. 6:06-mj-1146-Orl (M.D. Fla. June 6, 2006) (unpublished)	No, demands probable cause	District Court
<i>Spaulding Op.</i> , No. 06-1132-01 (M.D. Fla. May 25, 2006) (unpublished)	No, demands probable cause	Magistrate Judge (<i>aff'd mem.</i>)
D.C. Circuit		
<i>Facciola II Op.</i> , 407 F.Supp.2d 134 (D.D.C. 2006)	No, demands probable cause	Magistrate Judge
<i>Facciola I Op.</i> , 407 F.Supp.2d 132 (D.D.C. 2005)	No, demands probable cause	Magistrate Judge
<i>Robinson Op.</i> , 2005 WL 3658531 (D.D.C. Oct. 26, 2005)	No, demands probable cause	Magistrate Judge

4. Compelled Disclosure of Historical Cell-Site (or Satellite Phone) Location Information

Fortunately, the issue of government access to historical cell-site records has proven far less contentious than prospective collection. By a substantial majority, courts have held that such stored records may be obtained by means of a simple section 2703(d) order based upon the "specific and articulable facts" standard.[FN52] Significantly, even judges rejecting the hybrid theory have overwhelmingly endorsed the use of a 2703(d) order for historical records.[FN53]

a. Procedural issues

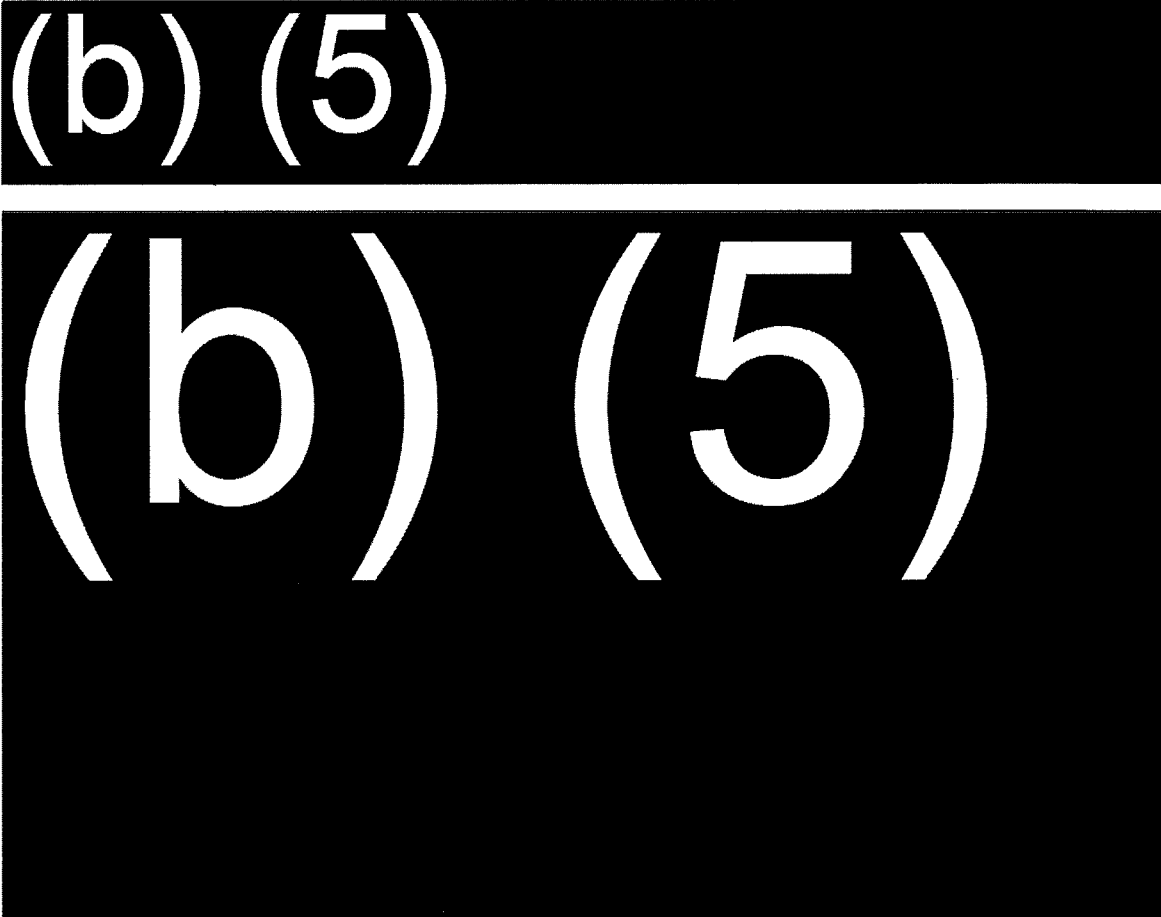
Prosecutors seeking section 2703(d) orders for historical cell-site information should be mindful of certain procedural issues:

- **required showing:** A section 2703(d) application should not merely certify that the requested records are relevant to an ongoing criminal investigation. Rather, the application should set forth "specific and articulable" facts in conformity with the statutory standard—making clear the relevance and materiality of the location information itself—and the order should make a specific finding that the application sets forth such facts.
- **requested information:** Prosecutors **should not** use section 2703(d) to request historical "GPS data," "E-911 information," "tower triangulation records," "location information derived from multiple towers simultaneously," or similar formulations.
- **"tower dumps":** Although requests for historical cell-site records will normally focus on a particular identified target phone, a request may instead focus on usage of a specific tower by *any* phone. For example, where a bank robber is observed making wireless calls during a robbery, contemporaneous records associated with the closest tower may assist in identifying the robber's phone, and thus the robber himself.[FN54]

Because these types of requests, sometimes referred to colloquially as "tower dumps," may produce substantial amounts of information, such requests should

seek records for a relatively narrow time frame. If the target's known calls can be characterized in objectively measurable terms—for example, calls of more than a certain length, or multiple outbound calls within a specified time frame—it is good practice to ask the provider to make selective disclosures after filtering out records not meeting those criteria.

b. Substantive objections (and responsive arguments)



5. Emergency Disclosures

Emergency disclosures of phone location information by a provider may fall into either of two categories: voluntary or compulsory.

a. Voluntary disclosure

Section 2702(c)(4) permits—but does not require—a service provider to disclose non-content subscriber records where the provider has a good-faith belief in the existence of "an emergency involving danger of death or serious physical injury to any person."

This provision clearly permits the disclosure of pre-existing information (that is, information already within the provider's possession at the time of the government request) such as historical cell-site records. The few cases on point also find that a provider may disclose *current* location information, including E-911 location data, in response to a kidnapping or other serious risk of harm.[FN58]

A separate provision, section 2702(c)(2), permits disclosures with the consent of

the subscriber. Such consent might be established through a provider's terms of service, or in some cases inferred from circumstances; most obviously, a kidnapping victim, injured hiker, or other person *in extremis* may reasonably be considered to have consented to release of location information pertaining to his or her phone. (A kidnapping victim cannot, of course, validly consent to the disclosure of location information on a kidnapper's phone.)

Note that when a provider makes a disclosure under any of the section 2702 exceptions, no followup legal process is required. Indeed, one court has expressly held that *nunc pro tunc* court authorization is not available under these circumstances.[FN59]

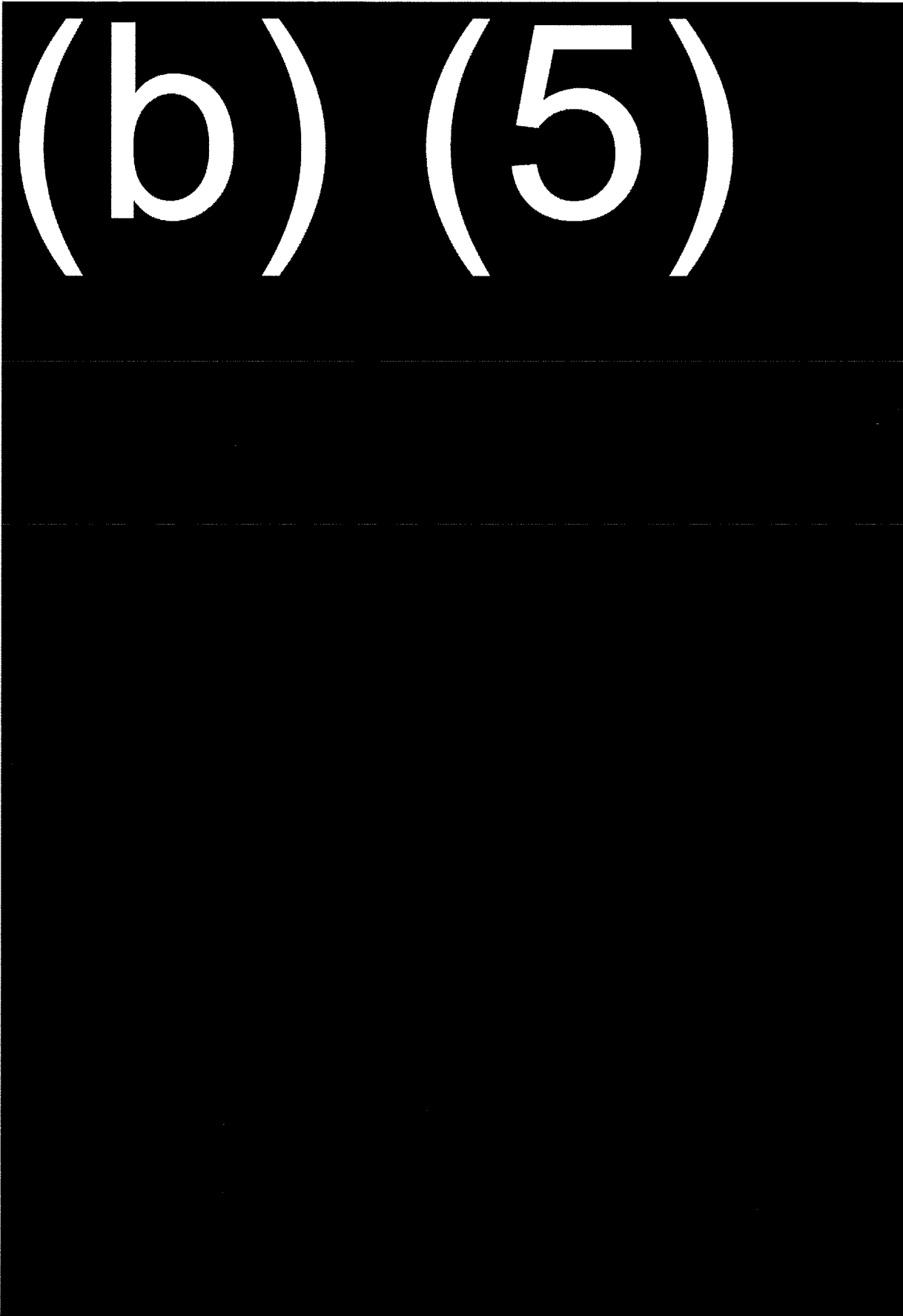
b. Compelled disclosure

Apart from the conventional legal mechanisms discussed above in section B, there are few options for emergency compulsion of wireless location information. Rule 41 makes no provision for *nunc pro tunc* issuance of a warrant,[FN60] and OEO strongly recommends against using the emergency provision of the pen/trap statute to obtain E-911/geolocation information, a practice explicitly rejected in several opinions.[FN61]

OEO does believe that the pen/trap emergency provision— 18 U.S.C. § 3125—may be used to obtain cell-site information in an emergency such as "immediate danger of death or serious bodily injury." [FN62] Reliance on this provision requires two critical steps. First, prior approval must be obtained from one of the statutorily prescribed officials; requests for these approvals should be made by an AUSA and coordinated through OEO's Electronic Surveillance Unit (reachable at 202-514-6809, or on nights/weekends through the Justice Command Center at 202-514-5000). Second, section 3125 requires that a followup application—in the case of cell-site information, for a hybrid order—be made within 48 hours after the pen/trap is initiated.

C. Responding to Suppression Motions

(b) (5)



(b) (5)

D. Comprehensive List of Federal Cases (as of August 2009)

Copies of any of the unpublished opinions listed below may be obtained from the author of this treatise.

In re Application, 2006 WL 2871743 (E.D. Wis. Oct. 6, 2006) (*Adelman Opinion*), *aff'g* 412 F.Supp.2d 947 (E.D. Wis. 2006) (*Callahan Opinion*)

In re Applications, 509 F.Supp.2d 64 (D. Mass. 2007) (*Alexander I Opinion*), *rev'd*, 509 F.Supp.2d 76 (D. Mass. 2007) (*Stearns Opinion*)

In re Applications, 530 F.Supp.2d 367 (D. Mass. 2007) (*Alexander II Opinion*)

In re Application, 402 F.Supp.2d 597 (D. Md. 2005) (*Bredar I Opinion*)

In re Application, 416 F.Supp.2d 390 (D. Md. 2006) (*Bredar II Opinion*)

In re Application, 439 F.Supp.2d 456 (D. Md. 2006) (*Bredar III Opinion*)

In re Application, 412 F.Supp.2d 947 (E.D. Wis. 2006) (*Callahan Opinion*), *aff'd*, 2006 WL 2871743 (E.D. Wis. Oct. 6, 2006) (*Adelman Opinion*)

In re Application, No. M-08-533 (E.D.N.Y. Jan. 12, 2009) (*Cogan Opinion*) (unpublished)

In re Application, 352 F.Supp.2d 45 (D. Mass. 2005) (*Collings Opinion*)

In re Application, 407 F.Supp.2d 132 (D.D.C. 2005) (*Facciola I Opinion*)

In re Application, 407 F.Supp.2d 134 (D.D.C. 2006) (*Facciola II Opinion*)

In re Application, Misc. No. 09-318 (D.D.C. June 15, 2009) (*Facciola III Opinion*) (unpublished)

In re Application, 415 F.Supp.2d 211 (W.D.N.Y. 2006) (*Feldman Opinion*)

In re Application, 2008 WL 5082506 (E.D.N.Y. Nov. 26, 2008) (*Garaufis I Opinion*)

In re Application, 2009 WL 1594003 (E.D.N.Y. Feb. 26, 2009) (*Garaufis II Op.*), *rev'g* 2009 WL 1530195 (E.D.N.Y. Feb. 12, 2009) (*Pollak Op.*)

In re Application, 405 F.Supp.2d 435 (S.D.N.Y. 2005) (*Gorenstein Opinion*)

In re Application, 2006 WL 6217584 (D.D.C. Aug. 25, 2006) (*Hogan Opinion*)

In re Application, No. S-06-SW-0041 (E.D. Cal. Mar. 15, 2006) (*Hollows I Opinion*) (unpublished)

In re Application, 2007 WL 397129 (E.D. Cal. Feb. 1, 2007) (*Hollows II Opinion*)

In re Application, 411 F.Supp.2d 678 (W.D. La. 2006) (*Hornsby Opinion*)

In re Application, 460 F.Supp.2d 448 (S.D.N.Y. 2006) (*Kaplan Opinion*)

In re Application, 2006 WL 1876847 (N.D. Ind. July 5, 2006) (*Lee Opinion*)

In re Application, 534 F.Supp.2d 585 (W.D. Pa. 2008) (*Lenihan Opinion*), *aff'd mem.* 2008 WL 4191511 (W.D. Pa. Sept. 10, 2008) (McVerry, J.), *appeal pending*

In re Application, 497 F.Supp.2d 301 (D.P.R. 2007) (*McGiverin Opinion*)

In re Application, 2009 WL 159187 (S.D.N.Y. Jan. 13, 2009) (*McMahon Opinion*)

In re Application, 396 F.Supp.2d 294 (E.D.N.Y. 2005) (*Orenstein Opinion*), *amending* 384 F.Supp.2d 562 (E.D.N.Y. 2005)

In re Application, 2007 WL 3341736 (S.D. Tex. Nov. 7, 2007) (*Owsley I Opinion*)

In re Application, 2007 WL 3342243 (S.D. Tex. Nov. 7, 2007) (*Owsley II Opinion*)

In re Application, 2007 WL3355602 (S.D. Tex. Nov. 8, 2007) (*Owsley III Opinion*)

In re Application, 2006 WL 468300 (S.D.N.Y. Feb. 28, 2006) (*Peck Opinion*)

In re Application, 2009 WL 1530195 (E.D.N.Y. Feb. 12, 2009) (*Pollak Op.*), *rev'd*, 2009 WL 1594003 (E.D.N.Y. Feb. 26, 2009) (*Garauffis II Op.*)

In re Application, No. 6:06-mj-1146-Orl (M.D. Fla. June 6, 2006) (*Presnell Opinion*) (unpublished)

In re Application, 2005 WL 3658531 (D.D.C. Oct. 26, 2005) (*Robinson Opinion*)

In re Application, 433 F.Supp.2d 804 (S.D. Tex. 2006) (*Rosenthal I Opinion*)

In re Application, 2007 WL 3036849 (S.D. Tex. Oct. 17, 2007) (*Rosenthal II Opinion*)

In re Application, 396 F.Supp.2d 747 (S.D. Tex. 2005) (*Smith I Opinion*)

In re Application, 441 F.Supp.2d 816 (S.D. Tex. 2006) (*Smith II Opinion*)

In re Application, 2007 WL 2086663 (S.D. Tex. July 6, 2007) (*Smith III Opinion*)

In re Application, No. 06-1132-01 (M.D. Fla. May 25, 2006) (*Spaulding Opinion*) (unpublished), *aff'd mem.* No. 06-1132-01 (M.D. Fla. June 15, 2006) (unpublished)

In re Application, 415 F.Supp.2d 663 (S.D. W. Va. 2006) (*Stanley Opinion*)

In re Applications, 509 F.Supp.2d 76 (D. Mass. 2007) (*Stearns Opinion*), *rev'g* 509 F.Supp.2d 64 (D. Mass. 2007) (*Alexander I Opinion*)

In re Application, No. 6:08-6038M-REW (E.D. Ky. Apr. 17, 2009) (unpublished) (*Weir Opinion*)

Jayne v. Sprint PCS, 2009 WL 426117 (E.D. Cal. Feb. 20, 2009)

United States v. Arthur, 2007 WL 2002500 (E.D. Mo. July 5, 2007)

United States v. Amaral-Estrada, 2006 WL 3197181 (S.D. Ind. June 30, 2006), *aff'd*, 509 F.3d 820 (7th Cir. 2007)

United States v. Flores, 2007 WL 2904109 (N.D. Ga. Sept. 27, 2007)

United States v. Forest, 355 F.3d 942 (6th Cir. 2004)

United States v. Navas, 2009 WL 1138020 (S.D.N.Y. Mar. 19, 2009)

United States v. Ortega-Estrada, 2008 WL 4716949 (N.D. Ga. Oct. 22, 2008)

United States v. Skinner, 2007 WL 1556596 (E.D. Tenn. May 24, 2007), *aff'd* 2007 WL 5238863 (E.D. Tenn. Apr. 26, 2007)

United States v. Suarez-Blanca, 2008 WL 4200156 (N.D. Ga. Mar. 26, 2008), *aff'd mem.*, No. 1:07-CR-23-TCB (N.D. Ga. June 30, 2008) (unpublished)

FN 1. See *United States v. Garcia-Alvarez*, 2007 WL 996162 at *1 (D.P.R. 2007) ("The location of the cell site for each call appears as a billing code in each customer's cell phone records.").

FN 2. See *U.S. Telecom Ass'n v. FCC*, 227 F.3d 450, 463 (D.C. Cir. 2000).

FN 3. See *In re Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems*, 15 FCC Rcd. 17442, 17462 (Sept. 8, 2000).

FN 4. See *FCC Amended Report to Congress on the Deployment of E-911 Phase II Services By Tier III Service Providers* at 1-2 (Apr. 1, 2005) ("*Phase II Deployment Report*"), available at http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-257964A1.pdf.

FN 5. See 47 C.F.R. § 20.18(h)(1)(i), (ii).

FN 6. See *Phase II Deployment Report* at 1-2, 7-11.

FN 7. See, e.g., *United States v. Ortega-Estrada*, 2008 WL 4716949 at *13 (N.D. Ga. Oct. 22, 2008) (phone GPS data accurate to 32 meters); *United States v. Louisuis*, 2006 WL 2193820 at *6 (M.D. Fla. 2006) (phone GPS data accurate to 40 meters).

FN 8. See *United States v. Ortega-Estrada*, 2008 WL 4716949 at *14 (N.D. Ga. Oct. 22, 2008) (ancillary request under Rule 41 as part of Title III wiretap order); *Hogan Opinion*, 2006 WL 6217584 at *3-4 (D.D.C. Aug. 25, 2006); *Smith I Opinion*, 396 F.Supp.2d 747, 749 & 765 (S.D. Tex. 2005) (application seeking prospective multiple-tower triangulation data misdescribed as "cell-site"). *But see Facciola III Opinion*, Misc. No. 09-318 at *3 (D.D.C. June 15, 2009) (unpublished) (insisting on invocation of All Writs Act, and not Rule 41, for order to obtain geolocation data on fugitive's phone).

FN 9. See, e.g., *United States v. Koyomejian*, 970 F.2d 536, 542 (9th Cir. 1992) (en banc).

FN 10. See *United States v. New York Tel. Co.*, 434 U.S. 159 (1977) (pre-dating enactment of pen register statute).

FN 11. 800 F.2d 1451, 1456 (9th Cir. 1986).

FN 12. See *United States v. Pangburn*, 983 F.2d 449, 455 (2d Cir. 1993).

FN 13. See 18 U.S.C. § 2518(8)(d), the constitutionality of which was upheld in *United States v. Cafaro*, 473 F.2d 489, 501 & n.9 (3d Cir. 1973) (citing numerous cases reaching the same conclusion).

FN 15. See *Garaufis I Opinion*, 2008 WL 5082506 at *7 (E.D.N.Y. Nov. 26, 2008); *cf. United States Telecom Ass'n v. FCC*, 227 F.3d 450, 463 (D.C. Cir. 2000) (holding that cell-site information is "signaling" information within the scope of CALEA).

FN 16. See *Cogan Opinion*, No. M-08-533 (E.D.N.Y. Jan. 12, 2009) (unpublished); *Garaufis I Opinion*, 2008 WL 5082506 (E.D.N.Y. Nov. 26, 2008); *Rosenthal II Opinion*, 2007 WL 3036849 (S.D. Tex. Oct. 17, 2007); *Kaplan Opinion*, 460 F.Supp.2d 448 (S.D.N.Y. 2006); *Rosenthal I*

Opinion, 433 F.Supp.2d 804 (S.D. Tex. 2006).

FN 17. See *Hollows II Opinion*, 2007 WL 397129 (E.D. Cal. Feb. 1, 2007); *Hornsby Opinion*, 411 F.Supp.2d 678 (W.D. La. 2006); *Hollows I Opinion*, No. S-06-SW-0041 (E.D. Cal. Mar. 15, 2006) (unpublished); *Gorenstein Opinion*, 405 F.Supp.2d 435 (S.D.N.Y. 2005).

FN 18. For a discussion of the opposing decisions (and the reasoning therein), see subsection B.3.b.

FN 19. See, e.g., *McMahon Opinion*, 2009 WL 159187 at *3 (S.D.N.Y. Jan. 13, 2009) ("locating the position of the phone, through the process of 'triangulation'"); *United States v. Amaral- Estrada*, 2006 WL 3197181 at *1 (S.D. Ind. June 30, 2006) ("a process of triangulation"); *Bredar I Opinion*, 402 F.Supp. 2d 597, 599 & n.4 (D. Md. 2005) (citing inappositely to FCC's E- 911 Phase II regulations imposing heightened precision requirements on GPS & triangulation methods).

FN 20. See *Lenihan Opinion*, 534 F.Supp.2d 585, 590 (W.D. Pa. 2008) (asserting without any support that tower information can reveal phone location to within 200 feet, narrowed even further via identification of specific face/sector carrying call).

FN 21. See, e.g., *McMahon Opinion*, 2009 WL 159187 at *5 (S.D.N.Y. Jan. 13, 2009); *Bredar I Opinion*, 402 F.Supp. 2d 597, 604-05 (D. Md. 2005).

FN 22. See *United States v. Suarez-Blanca*, 2008 WL 4200156 at *23 (N.D. Ga. Mar. 26, 2008), *aff'd mem.*, No. 1:07-CR-23- TCB (N.D. Ga. June 30, 2008) (unpublished); *Gorenstein Opinion*, 405 F.Supp.2d 435, 449-50 (S.D.N.Y. 2005).

FN 23. See *United States v. Miller*, 425 U.S. 435, 440 (1976) (bank's records "are not respondent's 'private papers'" but are "the business records of the banks" in which a customer "can assert neither ownership nor possession"); *SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743 (1984) ("when a person communicates information to a third party ... he cannot object if the third party conveys that information or records thereof to law enforcement authorities"); *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979) ("a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties").

FN 24. See *id.* at 715.

FN 25. *Id.* at 708.

FN 26. See, e.g., *Weir Opinion*, No. 6:08-6038M-REW at *20 (E.D. Ky. Apr. 17, 2009) (unpublished); *Garafis I Opinion*, 2008 WL 5082506 at *5 (E.D.N.Y. Nov. 26, 2008) (cell- site information, "unlike the information revealed by triangulation or ... Global Positioning System devices, is not precise enough to enable tracking of a telephone's movements within a home"); *McGiverin Opinion*, 497 F.Supp.2d 301, 311- 12 (D.P.R. 2007); *Hornsby Opinion*, 411 F.Supp.2d 678, 682 (W.D. La. 2006) ("[C]ell-site information ... does not permit detailed tracking of a cell phone user within any residence or building. Indeed, the Government will not be able to pinpoint which room, house or building (if any) the user is in."); *Gorenstein Opinion*, 405 F.Supp.2d 435, 449 (S.D.N.Y. 2005).

FN 27. See, e.g., *Lenihan Opinion*, 534 F.Supp.2d 585, 595 & 602 (W.D. Pa. 2008); *Orenstein Opinion*, 396 F.Supp. 2d 294, 321 (E.D.N.Y. 2005); *Smith I Opinion*, 396 F.Supp. 2d 747, 757 (S.D. Tex. 2005).

FN 28. See, e.g., *Weir Opinion*, No. 6:08-6038M-REW at *13- 14 (E.D. Ky. Apr. 17, 2009) (unpublished); *Stearns Opinion*, 509 F.Supp.2d 76, 81 n.11 (D. Mass. 2007); *Kaplan Opinion*, 460 F.Supp.2d 448, 461 (S.D.N.Y. 2006) ("Here, the government does not seek to *install* any sort of tracking device") (emphasis in original); *Hornsby Opinion*, 411 F.Supp.2d 678, 681 (W.D. La. 2006) ("The existence of a true 'tracking device' is unknown to, and cannot be disabled or turned off by, the person being tracked."); *Gorenstein Opinion*, 405 F.Supp.2d 435, 449 n.8 (S.D.N.Y.

2005) (section 3117 "contemplates the 'installation' of a tracking device, which has not been sought here").

FN 29. See H.R. Rep. No. 467, 99th Cong., 2d Sess. at 60 (1986).

FN 30. "[T]he term 'tracking device' means an electronic or mechanical device which permits the tracking of the movement of a person or object." 18 U.S.C. § 3117(b).

FN 31. See *Hollows Opinion*, 2007 WL 397129 at *2 (E.D. Cal. Feb. 1, 2007).

FN 32. See, e.g., *United States v. Gbemisola*, 225 F.3d 753, 758 (D.C. Cir. 2000) ("But by contrast to statutes governing other kinds of electronic surveillance devices, section 3117 does not **prohibit** the use of a tracking device in the absence of conformity with the section.") (emphasis in original); *Gorenstein Opinion*, 405 F.Supp.2d 435, 449 n.8 (S.D.N.Y. 2005) (same).

FN 33. Fed. R. Crim. P. 41, advisory committee's note, subd. (b) (2006).

FN 34. The Supreme Court expressly reserved decision on this question in *Karo*. See 468 U.S. at 718 n.5 (declining to rule on whether "reasonable suspicion" would suffice).

FN 35. Fed. R. Crim. P. 41, advisory committee's note, subd. (b) (2006); see also *Kaplan Opinion*, 460 F.Supp.2d 448, 461 (S.D.N.Y. 2006); *Gorenstein Opinion*, 405 F.Supp. 2d 435, 449 n.8 (S.D.N.Y. 2005).

FN 36. See, e.g., *McGiverin Opinion*, 497 F.Supp.2d 301, 310- 11 (D.P.R. 2007).

FN 37. 18 U.S.C. § 2510(12)(C).

FN 38. A "wire communication" must contain an "aural transfer," *i.e.*, the human voice. See 18 U.S.C. § 2510(1), (18).

FN 39. See 18 U.S.C. §§ 2510(15) & 2711(1); *Kaplan Opinion*, 460 F.Supp.2d 448 (S.D.N.Y. 2006) ("Cell phone service providers clearly fit within this definition.").

FN 40. See *Gorenstein Opinion*, 405 F.Supp.2d 435, 444 (S.D.N.Y. 2005).

FN 41. See, e.g., *McMahon Opinion* 2009 WL 159187 (S.D.N.Y. Jan. 13, 2009) ("a provider of CSLI [cell-site location information] does not fall within the statutory definition of "electronic communications [*sic*] service").

FN 42. *Lenihan Opinion*, 534 F.Supp.2d 585, 604 (W.D. Pa. 2008) (emphasis in original).

FN 43. *Gorenstein Opinion*, 405 F.Supp.2d 435, 446 (S.D.N.Y. 2005) (emphasis added).

FN 44. See *McMahon Opinion*, 2009 WL 159187 at *5-6 (S.D.N.Y. Jan. 13, 2009).

FN 45. Moreover, in many cases the provider may not have **any** named subscriber for a given phone, as in the case of prepaid phones sold as commodities.

FN 46. OEO does not believe that "subscriber" in section 1002(a)(2) (or in ECPA) should be read so narrowly. *But see Stanley Opinion*, 415 F.Supp.2d 663, 666 (S.D. W. Va. 2006) (where fugitive was using another person's cell phone, pen/trap order seeking cell-site information was granted because "[t]he user of a cellphone who is *not* the subscriber has no protection" under 47 U.S.C. § 1002) (emphasis in original).

FN 47. See, e.g., *McGiverin Opinion*, 497 F.Supp.2d 301, 306 (D.P.R. 2007) (citing cases).

FN 48. See, e.g., *Orenstein Opinion*, 396 F.Supp.2d 294, 308- 09 (E.D.N.Y. 2005).

FN 49. *Gorenstein Opinion*, 405 F.Supp.2d 435, 448 (S.D.N.Y. 2005); see also *Kaplan Opinion*, 460 F.Supp.2d 448, 459-60 (S.D.N.Y. 2006) ("It makes sense that the Pen Register Statute would provide the procedural framework").

FN 50. See *McGiverin Opinion*, 497 F.Supp.2d 301, 309 (D.P.R. 2007); *Adelman Opinion*, 2006 WL 2871743 (E.D. Wis. Oct. 6, 2006).

FN 51. *Smith II Opinion*, 441 F.Supp.2d 816, 834-35 (S.D. Tex. 2006) (emphasis in original).

FN 52. See *United States v. Suarez-Blanca*, 2008 WL 4200156 at *32 (N.D. Ga. Mar. 26, 2008), *aff'd mem.*, No. 1:07-CR-23- TCB (N.D. Ga. June 30, 2008) (unpublished); *Stearns Opinion*, 509 F.Supp.2d 76 (D. Mass. 2007); *Rosenthal II Opinion*, 2007 WL 3036849 at *5 (S.D. Tex. Oct. 17, 2007); *United States v. Arthur*, 2007 WL 2002500 (E.D. Mo. July 5, 2007); *Hogan Opinion*, 2006 WL 6217584 at *2 n.3 (D.D.C. Aug. 25, 2006) (in dicta).

FN 53. See *Weir Opinion*, No. 6:08-6038M-REW at *12 & *15 (E.D. Ky. Apr. 17, 2009) (unpublished); *Alexander II Opinion*, 530 F.Supp.2d 367 (D. Mass. 2007); *Feldman Opinion*, 415 F.Supp.2d 211, 214 (W.D.N.Y. 2006) (in dicta); *Smith I Opinion*, 396 F.Supp.2d 747, 748 (S.D. Tex. 2005); *Orenstein Opinion*, 396 F.Supp.2d 294, 313 (E.D.N.Y. 2005) (in dicta).

FN 54. See, e.g., *United States v. Duffey*, 2009 WL 2356156 at *1 (N.D. Tex. July 30, 2009).

FN 55. See *Stearns Opinion*, 509 F.Supp.2d 76 (D. Mass. 2007), *rev'g* 509 F.Supp.2d 64 (D. Mass. 2007) (*Alexander I Opinion*); *Rosenthal II Opinion*, 2007 WL 3036849 at *5 (S.D. Tex. Oct. 17, 2007).

FN 56. See *Lee Opinion*, 2006 WL 1876847 (N.D. Ind. July 5, 2006).

FN 57. See *Lenihan Opinion*, 534 F.Supp.2d 585 (W.D. Pa. 2008), *appeal pending*.

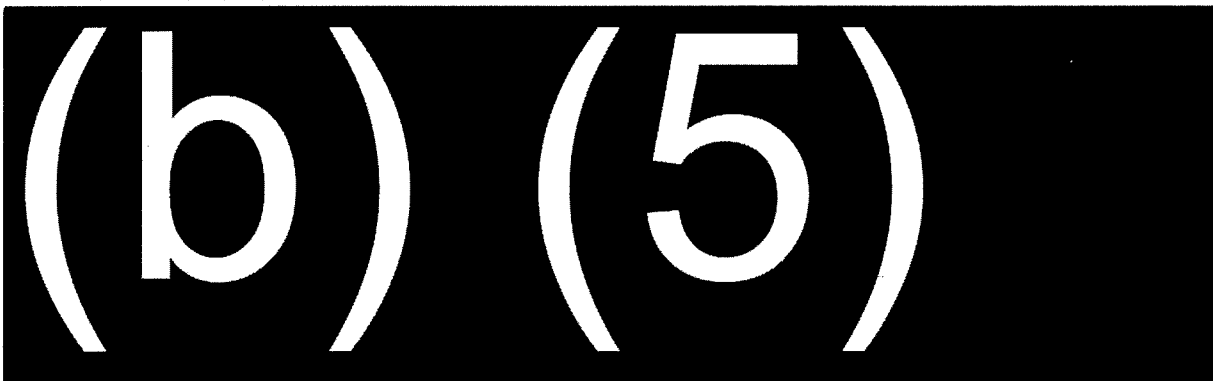
FN 58. See *Jayne v. Sprint PCS*, 2009 WL 426117 at *6-7 (E.D. Cal. Feb. 20, 2009) (disclosure of GPS data in alleged kidnapping situation); *Collings Opinion*, 352 F.Supp.2d 45 (D. Mass. 2005) (disclosure of unspecified records in kidnapping situation).

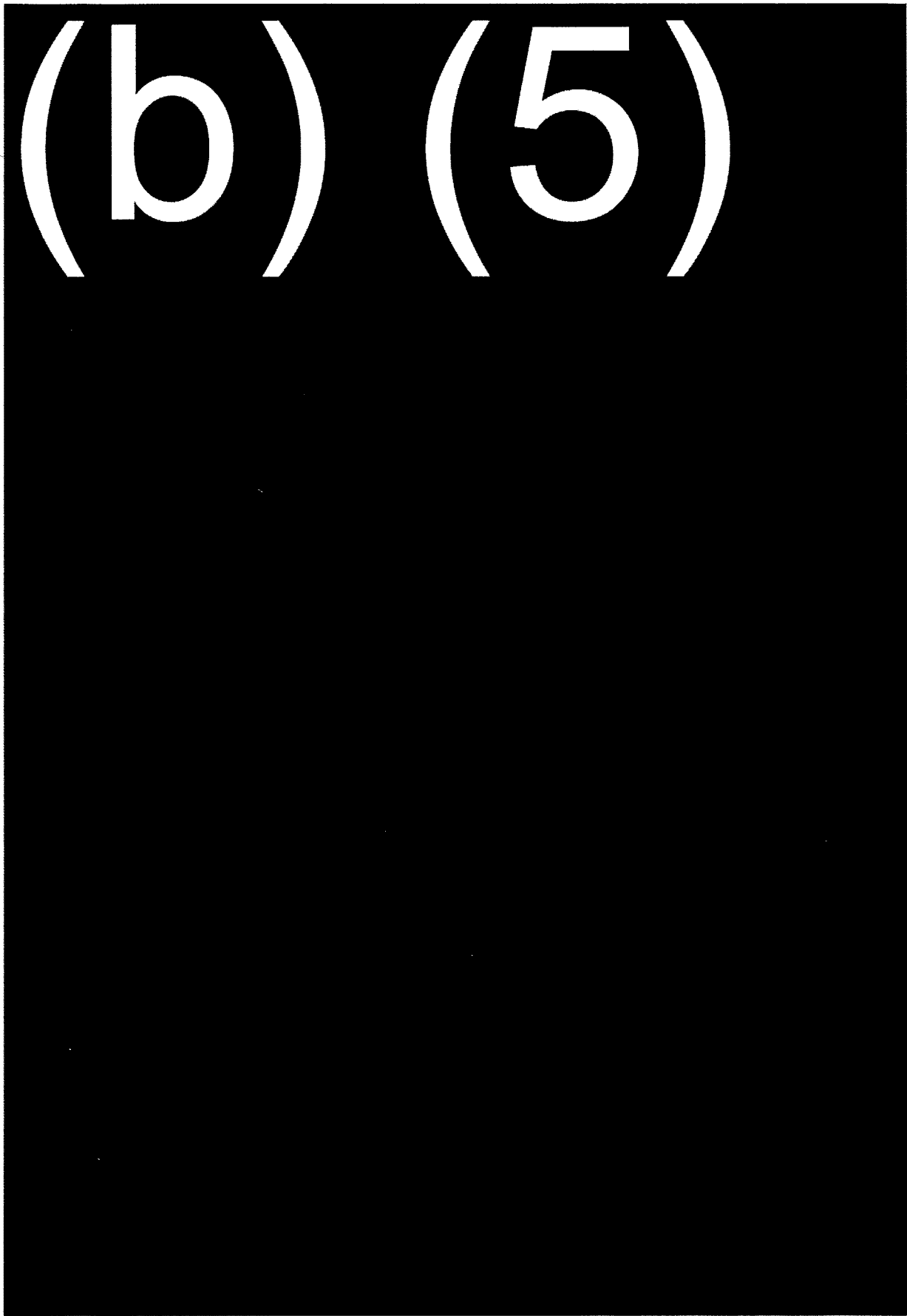
FN 59. See *Collings Opinion*, 352 F.Supp.2d 45, 47 (D. Mass. 2005).

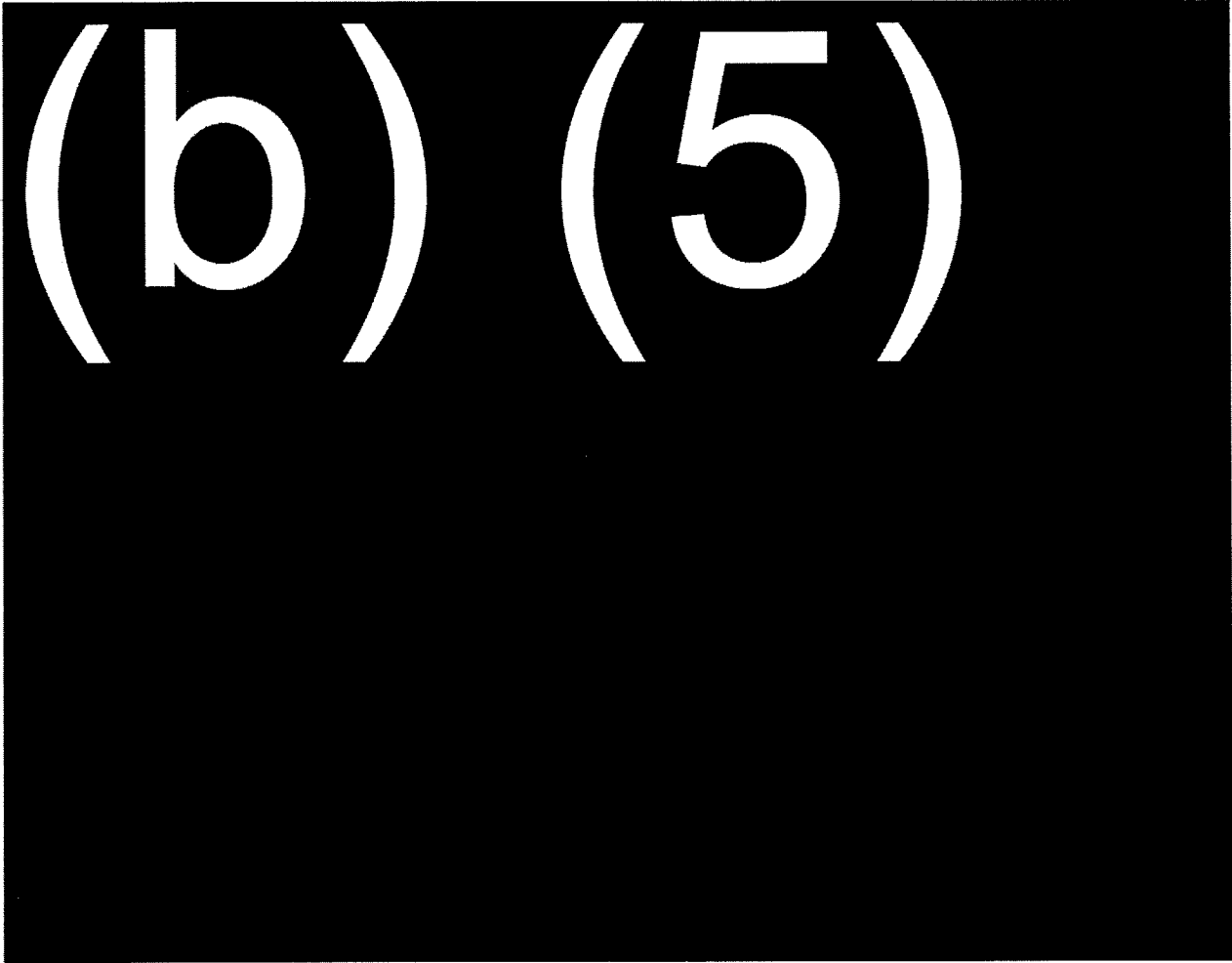
FN 60. Note, however, that Rule 41(d)(3) & (e)(3) allows for issuance of telephonic warrants where time is of the essence.

FN 61. See *Owsley I Opinion*, 2007 WL 3341736 (S.D. Tex. Nov. 7, 2007); *Owsley II Opinion*, 2007 WL 3342243 (S.D. Tex. Nov. 7, 2007); *Owsley III Opinion*, 2007 WL3355602 (S.D. Tex. Nov. 8, 2007); *Smith III Opinion*, 2007 WL 2086663 (S.D. Tex. July 6, 2007).

FN 62. § 3125(a)(1)(A).







USABook > Electronic Surveillance > Tracking Devices Manual > **Part II.**
prev | next | help | download

Red alert!!! In *United States v. Jones*, 2012 WL 171117 (U.S. Jan. 23, 2012), the Supreme Court held that "the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a search" within the meaning of the Fourth Amendment. See the February 27, 2012, Appellate Section Guidance Memorandum.

Part II:

Mobile Tracking Devices

- A. Technology Basics
- B. Controlling Supreme Court Precedents: Knotts and Karo
- C. Determining Whether Court Authorization is Necessary
 1. Installation and Removal
 2. Authority to Monitor
- D. Obtaining Court Authorization to Install and/or Monitor a Tracking Device
 1. Venue: where to apply?
 2. Time limits: installation timing and overall duration of the order
 3. Authority to enter private areas or move vehicles
 4. The return
 5. Service of notice, and delay thereof
 6. Extensions/renewals
 7. AO Forms
- E. Responding to Suppression Motions

A. Technology Basics

Originally, mobile tracking devices were simple radio "beepers" transmitting on a known frequency. After surreptitiously installing a beeper in or on the item to be tracked, agents could determine the direction of the signal's source using radio monitoring equipment and, by following that signal, the beeper's location. This process required the agents to be in reasonable proximity to the device; in the absence of a signal, no tracking was possible.

Current devices used by law enforcement use a variety of more advanced technologies. Instead of simply emitting a radio beacon, modern tracking devices often calculate their own approximate position using signals from navigational satellite systems. Law enforcement devices using the most well-known of these, the Global Positioning System (GPS) satellite constellation, can provide location data accurate to approximately 100 feet. Less expensive devices may instead rely on the Polar Operational Environmental Satellite system (POES) operated by the National Oceanic and Atmospheric Administration, providing accuracy in the range of one-half mile. In either case, reduced satellite visibility—such as when a tracking device enters a building—may adversely affect the accuracy or availability of location reporting.

Many current devices incorporate the ability to report location data at regular intervals using cellular Short Message Service (SMS) text messaging. When these devices move out of cellular coverage and are unable to report in real time, they buffer the data for later reporting when cellular coverage again becomes available.

Tracking devices may have capabilities in addition to reporting location data. In particular, so-called "activation" or "trigger" devices can report the occurrence of a physical event such as the

opening of a package or other object containing the device.[FN1]

B. Controlling Supreme Court Precedents: *Knotts* and *Karo*

Any legal analysis of tracking devices necessarily begins with the landmark decisions in *United States v. Knotts*[FN2] and *United States v. Karo*. [FN3] Because the Supreme Court has not revisited the legal implications of tracking devices in the intervening quarter century, these two cases continue to define the Fourth Amendment boundaries in this area.

Knotts and *Karo* proceed from nearly identical initial settings. In each case, investigators suspected the defendant of manufacturing or trafficking in illegal narcotics; determined that each intended to purchase drums of chemicals (chloroform and ether, respectively) to be used in processing the narcotics; and, with the consent of the chemical vendor, installed a radio "beeper" in a drum of chemicals subsequently delivered to the defendant.[FN4] At this point, however, the factual settings diverge.

In *Knotts*, officers followed the purchaser of the drum of chloroform, maintaining contact with his car both by direct visual surveillance and by monitoring the beeper signals. When the purchaser transferred the drum to a confederate's car, officers pursued that vehicle until its driver successfully executed evasive maneuvers. Despite losing visual contact, the officers were thereafter able to monitor "the approximate location" of the beeper's signal, which led them to a remote cabin later revealed to contain a clandestine drug laboratory. Crucially, the Court observed that "[t]he record before us does not reveal that the beeper was used after the location in the area of the cabin had been initially determined." [FN5]

In appealing his subsequent conviction, *Knotts* claimed that the monitoring of the beeper violated his Fourth Amendment reasonable expectation of privacy. (Notably, he did not challenge the warrantless installation.[FN6]) For several reasons, the Court emphatically rejected his argument, beginning with the observation that "[a] person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another." [FN7] The Court attached no importance to the fact that the officers had not themselves maintained continuous visual contact, holding it legally sufficient that a hypothetical officer could have done so from lawful vantage points, and declaring that "[n]othing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case." [FN8]

The Court extended this reasoning to the tracking that led investigators to the cabin, reversing the court of appeals and holding that "[a] police car following [the confederate] at a distance throughout his journey could have observed him leaving the public highway and arriving at the cabin." [FN9] In finding no constitutional infirmity, the Court placed great emphasis on the fact that the beeper monitoring led only to the general vicinity of the cabin: "there is no indication that the beeper was used in any way to reveal information as to the movement of the drum within the cabin, or in any way that would not have been visible to the naked eye from outside the cabin." [FN10]

In *Karo*, the Court faced an appreciably more complex set of facts. Monitoring the beeper in the can of ether without a valid warrant,[FN11] agents tracked it to three successive houses, two commercial storage facilities, and thence (using both visual and beeper surveillance) to two more residences, the last one in Taos. Upon seeking a warrant for the Taos residence—relying in part on the beeper monitoring results to establish probable cause—the government conducted a search and discovered cocaine and laboratory equipment.[FN12]

Unlike *Knotts*, the defendants in *Karo* objected to the warrantless installation. The Court made short work of this argument, holding that because the installation occurred with the consent of the lawful owner (the vendor who happened to be an informant), neither the installation *per se* nor the subsequent transfer of the rigged can constituted a Fourth Amendment search or seizure. On the latter point, the Court cited its prior definition of a seizure as a "meaningful interference with an individual's possessory interests in [...] property." [FN13] Finding that the beeper's non-destructive (albeit

technically trespassory) presence did not rise to the level of a "meaningful interference," the Court accordingly rejected Karo's claim.

However, the Court reached a different conclusion with respect to the government's subsequent monitoring of the beeper. First, the Court noted that only via electronic surveillance—and not by additional means such as visual observation—the government determined positively both that the ether had been moved from a vehicle into the Taos residence, and that it remained there over time. [FN14] Contrasting these facts with those in *Knotts*, the Court held that the monitoring "reveal[ed] a critical fact about the interior of the premises that the Government ... could not have otherwise obtained without a warrant." [FN15]

Having thus found the monitoring of the beeper inside the Taos residence improper, the Court determined that the warrant to search that house was nevertheless based on adequate untainted evidence. Specifically, the Court found that the tracking of the beeper up to its arrival at the Taos residence was proper. In reaching this conclusion, the Court established two important legal principles.

First, the Court held that the earlier, presumably unlawful monitoring of the beeper did not preclude admissibility of evidence obtained from its use at later times:

Assuming for present purposes that prior to its arrival at the second warehouse the beeper was illegally used to locate the ether in a house or other place in which [defendants] had a justifiable claim to privacy, we are confident that such use of the beeper does not taint its later use in locating the ether and tracking it to Taos. The movement of the ether from the first warehouse was undetected, but by monitoring the beeper the agents discovered that it had been moved to the second storage facility. No prior monitoring of the beeper contributed to this discovery; using the beeper for this purpose was thus untainted by any possible prior illegality. [FN16]

Thus, *Karo* explicitly stands for the proposition that where a tracking device is lawfully installed, suppression will apply only to the specific times (if any) when the device is monitored without a warrant and reveals private facts about the interior of a protected area.

Second, the Court made clear that tracking device monitoring is a Fourth Amendment "search" only where it reveals information about the interior of a *specific* protected area:

[T]he beeper informed the agents only that the ether was somewhere in the [storage facility] warehouse; it did not identify the specific locker in which the ether was located. Monitoring the beeper revealed nothing about the contents of the locker that [defendants] had rented and hence was not a search of that locker. [Footnote:] Had the monitoring disclosed the presence of the container within a particular locker the result would be otherwise, for surely [defendants] had a reasonable expectation of privacy in their own storage locker. [FN17]

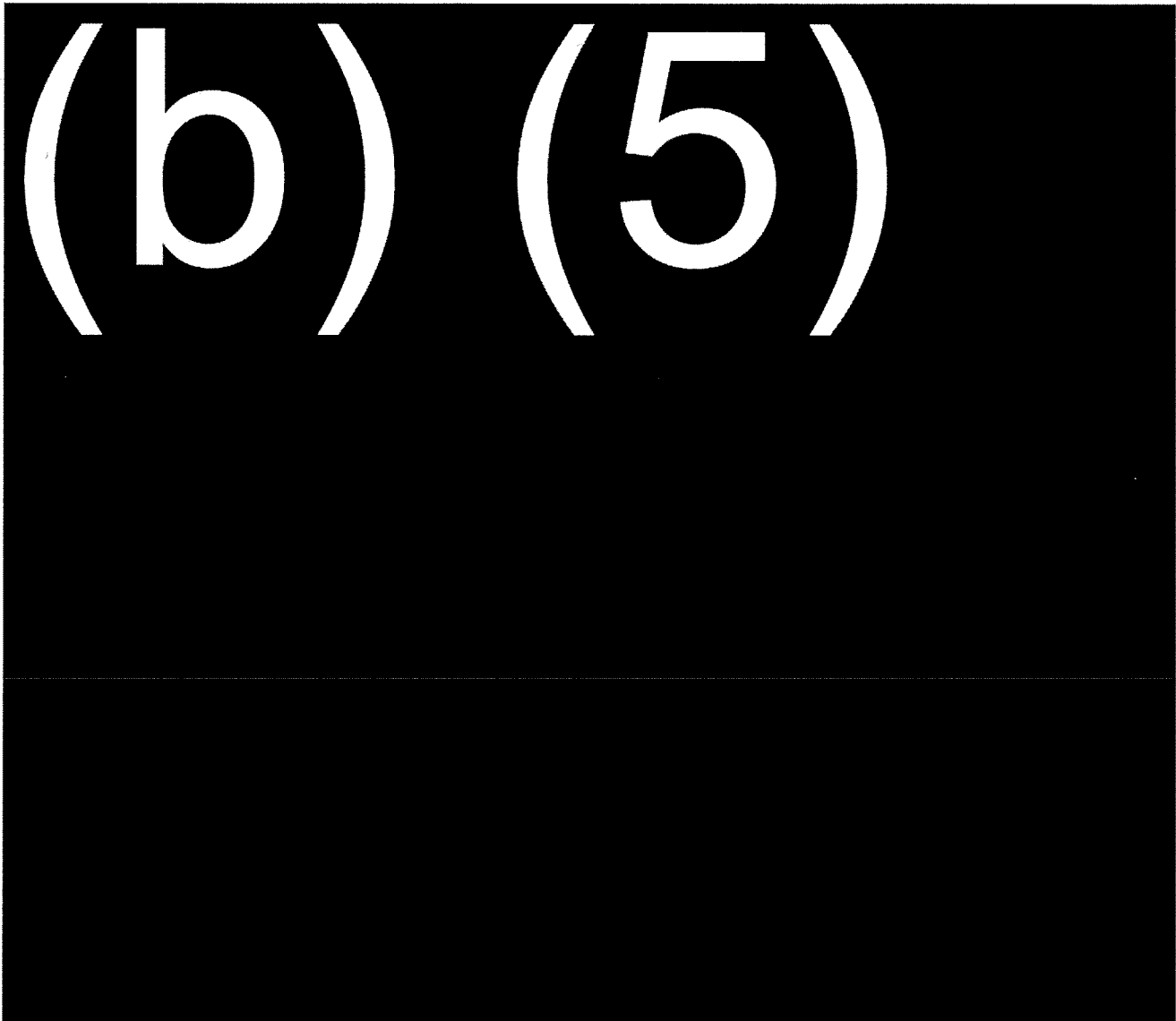
Thus, the Fourth Amendment test under *Karo* is not simply whether the tracked object is inside a protected private location. (That is a necessary but not sufficient condition.) Rather, to perform a "search" the government must learn which particular private space the tracked object is in, and do so solely by means of monitoring the tracking device. If the tracking device reveals only general location information (*i.e.*, does not disclose the tracked object's presence inside a specific protected area), agents are free to use that information, even if other lawful techniques eventually narrow the tracked item to a specific private space. [FN18]

C. Determining Whether Court Authorization is Necessary

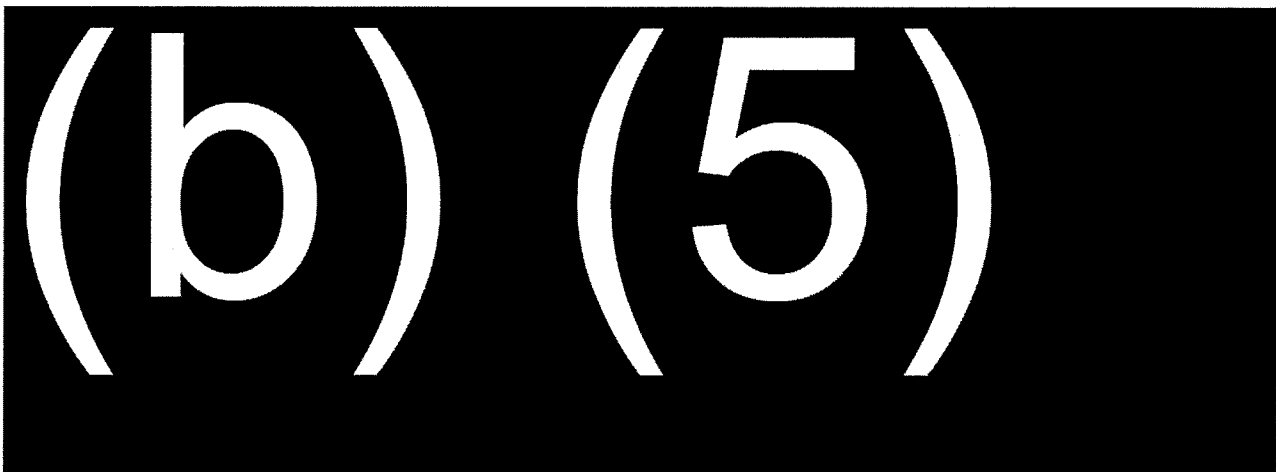
In light of *Karo*'s determination that the use of a tracking device may infringe upon a reasonable expectation of privacy, prosecutors and agents should carefully consider the following factors in determining whether they need to obtain a warrant. In particular, both the installation of the device and its planned subsequent monitoring must be separately analyzed for Fourth Amendment

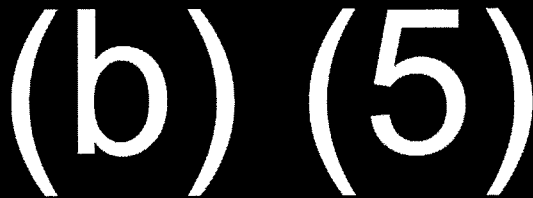
Implications.

1. Installation and Removal



2. Authority to Monitor





D. Obtaining Court Authorization to Install and/or Monitor a Tracking Device

In the years following *Karo*, law enforcement relied upon Rule 41 as the source of authority for court orders relating to the installation and monitoring of tracking devices.[FN34] This is unremarkable, given that courts have found Rule 41 an appropriate means of authorizing other types of ongoing surveillance—surreptitious video surveillance[FN35] and pen registers[FN36]—not expressly mentioned in the text of the Rule. (Note also that tracking device communications are excluded from the reach of the wiretap statute.[FN37])

Effective December 1, 2006, however, Rule 41 contains explicit provisions for the issuance of tracking device warrants. The addition of this language does not mean that a warrant is required whenever a tracking device is used; as the 2006 Advisory Committee Note makes clear, the amendment does nothing to alter the rule that "[i]f ... the officers intend to install and use the device without implicating any Fourth Amendment rights, there is no need to obtain the warrant." [FN38]

Prosecutors and agents planning to obtain a Rule 41 tracking device warrant should be mindful of the following procedural issues:

1. Venue: where to apply?

Rule 41(b)(4) provides that a court may issue a warrant to install a tracking device within the court's jurisdiction, and for tracking of that device both within and outside the district. (This provision restates 18 U.S.C. § 3117(a), which is now essentially superfluous.) Thus, application should be made in the district where the installation will occur.

2. Time limits: installation timing and overall duration of the order

In addition to requiring specification of the person or property to be tracked and the magistrate judge to whom the warrant must be returned, Rule 41(e)(2)(B) imposes three time-related limits on tracking device warrants. First, it requires that the warrant command the officer to perform the installation within 10 calendar days. Second, the warrant must command the installation to be done in daytime hours[FN39] absent explicit authorization, for good cause shown, to install at other times. Third, the period of monitoring may not exceed 45 days from the date of issuance.

A note of caution on this last point: the 45-day limit is an absolute ceiling, and includes the period between issuance of the warrant and installation of the device. In this respect, tracking device warrants are unlike wiretap orders, where the authorized period of monitoring begins to run only on the earlier of a) the tenth day after issuance or b) commencement of monitoring.[FN40]

3. Authority to enter private areas or move vehicles

As discussed above in section C.1, the installation of a tracking device may entail entry into or onto a protected area (such as the interior of a vehicle or private residential garage) or even moving a vehicle temporarily. Subsequent maintenance of the device, such as to repair a malfunction or replace a dead battery, or its eventual removal may raise the same issue. According to the 2006 Advisory Committee Note, Rule 41 permits a court to authorize these kinds of entries/access.[FN41]

OEO recommends that applicants seeking such authorization specify with particularity the location

(s) to be entered. We strongly advise against seeking blanket authorization to enter any private location without limitation where the vehicle (or other item to be tracked) may be found in the future, as such an order would raise significant constitutional questions.

4. The return

Rule 41(f)(2) requires a tracking device warrant to be returned within calendar 10 days after use of the device has ended. As set out in the Rule, the officer should indicate "the exact date and time the device was installed and the period during which it was used."

5. Service of notice, and delay thereof

By default, Rule 41(f)(2)(C) requires that notice be provided to "the person who was tracked or whose property was tracked" within 10 calendar days after the use of the tracking device ends. Service may be made personally, or by leaving a copy at the person's residence in combination with service by mail.

Subsections (f)(2)(C) and (f)(3) both refer somewhat obliquely to statutory authority to delay the service of notice. As the 2006 Advisory Committee Note makes clear, 18 U.S.C. § 3103a(b) is the appropriate mechanism.[FN42]

Under that statute, notice may be delayed for any of the reasons listed separately in 18 U.S.C. § 2705 (except for undue delay of a trial), such as the risk of flight, destruction of evidence, or witness intimidation. By default, an initial delay may run for up to 30 days, and extensions for up to 90 days. Where the facts of the case justify delay, however, a court may deviate from these default periods.

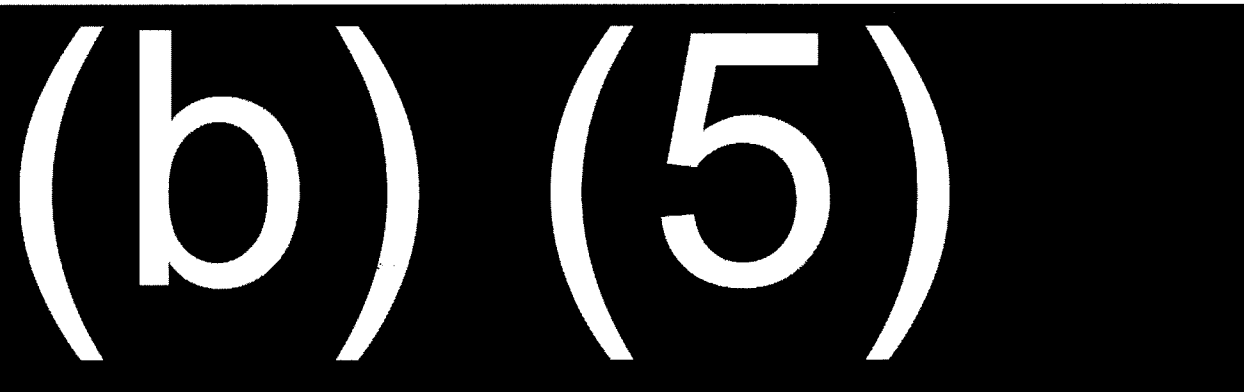
6. Extensions/renewals

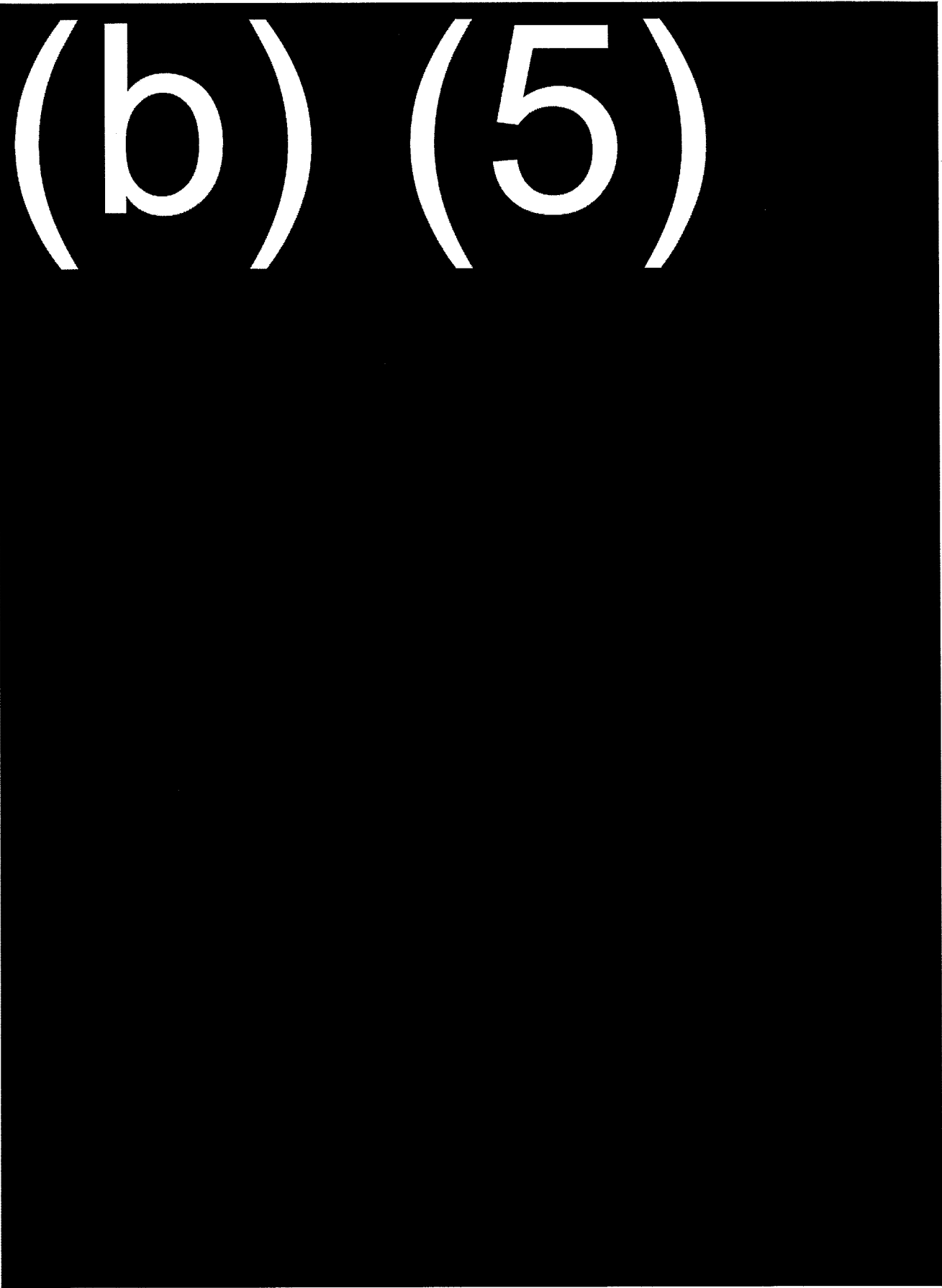
On its face, Rule 41(e)(2)(B) permits a tracking device warrant to be extended/renewed "for good cause." OEO strenuously advises against applying this standard, and emphatically recommends that any extension application not only set forth, but affirmatively declare that it is setting forth, the same showing as in the original application. Similarly, the extension order/warrant should include a corresponding statement of the showing made. Under normal circumstances, that will involve a new showing of probable cause based upon additional facts.[FN43]

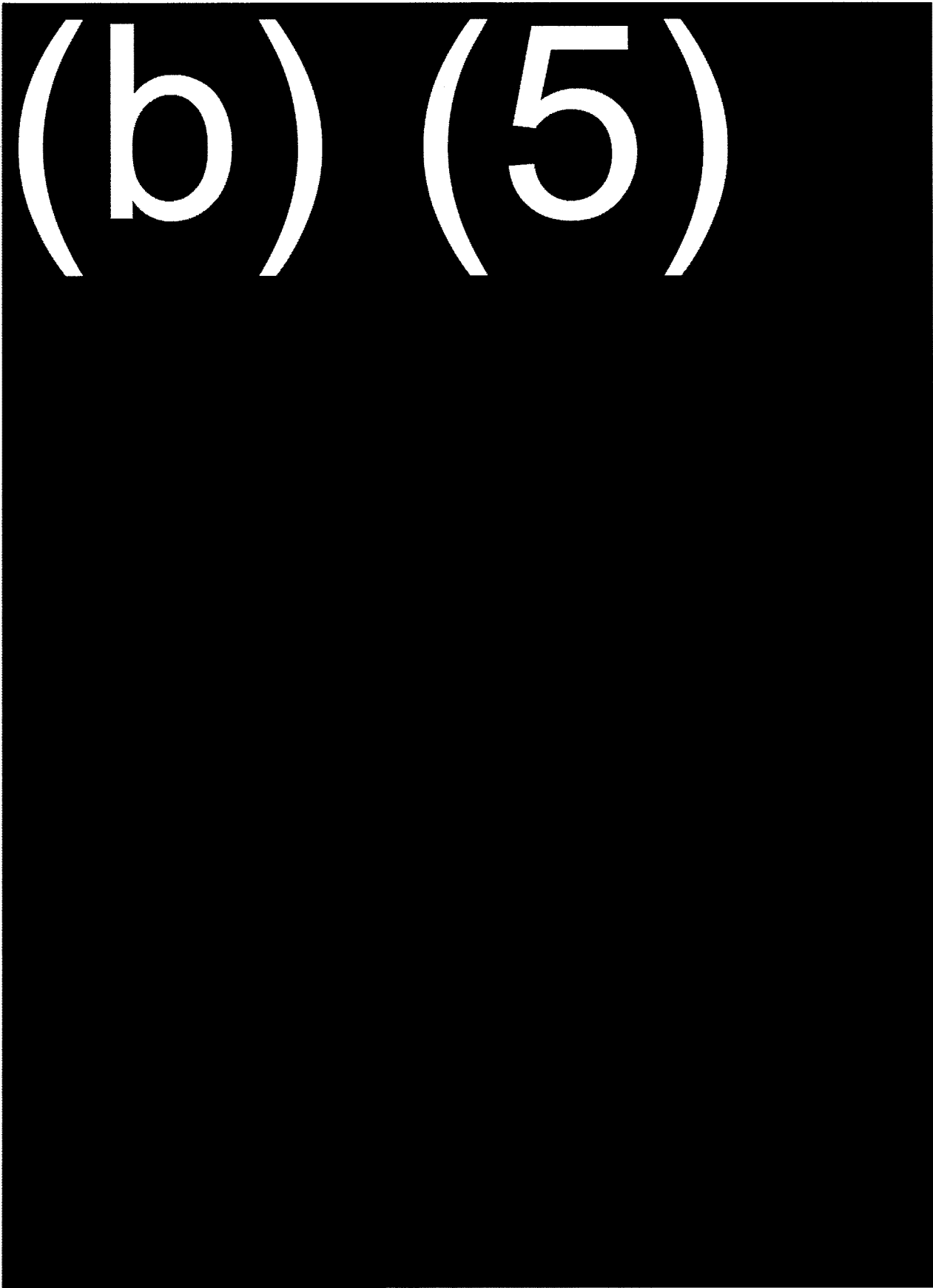
7. AO Forms

In January 2009, the Administrative Office of the United States Courts issued new forms (102 through 104) for use in seeking a tracking device warrant. Because these forms contain a number of errors—*e.g.*, conflating "execution" and "installation," and adding requirements for the return beyond those set out in Rule 41—OEO suggests using the attached forms instead. (Forms 102-104 should not be used to obtain location data from an OnStar device or a target's own cell phone, as neither scenario involves the "installation" of a "tracking device" within the meaning of the rule.)

E. Responding to Suppression Motions







(b) (5)

CRM-0036

(b) (5)

USABook > Electronic Surveillance > Tracking Devices Manual > **Part III.**
prev | next | help | download

Part III:

Telematics Providers (OnStar, etc.)

- A. Technology Basics
- B. Procedural Issues

A. Technology Basics

In recent years, vehicle telematics systems—integrated electronic devices providing an array of communication and navigation functions—have become increasingly common in the United States and abroad. Of these, the OnStar system developed by General Motors vehicles is probably the most well known, although Mercedes-Benz TeleAid and BMW Assist (both operated by ATX Technologies) also command U.S. market share. Available services typically include such options as "concierge" service (on-demand wireless communications with a company operator to request roadside or other assistance), automatic emergency service response by a company operator (triggered by airbag deployment or other crash sensors), and stolen vehicle location detection.

In providing many of these services, a telematics system relies upon two essential components: an on-board Global Positioning System (GPS) device and wireless communications equipment. The GPS device provides the capability of determining the vehicle's location. The wireless communications device—in essence, a built-in cellular phone—enables voice and data transmissions from the vehicle to the telematics provider or, in many cases, to any other device on the public switched telephone network.

From a law enforcement perspective, these features provide at least two separate avenues for obtaining location information. First, because the wireless communications capability relies on conventional cellular service,[FN1] investigators may obtain the same types of location records—such as historical and prospective cell-site data—available for handheld cellular phones. (See Part I for a complete discussion.) In addition, the telematics provider may be able to provide a target vehicle's current location[FN2] as computed by the on-board vehicle GPS system.

B. Procedural Issues

To obtain location information associated with a telematics system's wireless service, prosecutors should use the procedures described in Part I. Legal process should be directed at the wireless carrier (e.g., Verizon Wireless for OnStar customers) and should specify the 10-digit telephone number associated with the customer's service.

To obtain real-time GPS location information computed by a vehicle's on-board GPS system, OEO recommends the use of a Rule 41 warrant. (See the model forms in the Appendix.) For the same reasons applicable to cell phone location requests[FN3]—including the fact that the government performs no "installation" when making use of a telematics system's location-finding capabilities—OEO recommends taking the position that a telematics system is not a "tracking device" within the meaning of 18 U.S.C. § 3117 or Rule 41.[FN4]

Rule 41(b)(2) states that a warrant may issue for "a person or property outside the district if [it] is located within the district when the warrant is issued." As a result, OEO suggests that the best practice is to obtain the warrant in the district where the vehicle is known or reasonably believed to be. (This is not altogether paradoxical: the vehicle's general whereabouts might be determined from cell-site data, visual sightings, or other sources such as a confidential informant.) In the alternative, the warrant may be sought in the district where the telematics service provider is located—for example,

OnStar's headquarters in the Eastern District of Michigan—or where its employees will perform the actions necessary to determining the vehicle's location.

FN 1. For example, OnStar devices are served by Verizon Wireless.

FN 2. Telematics systems do not typically retain historical GPS data reflecting a vehicle's past movements.

FN 3. See Part I.B.3.b.

FN 4. Note that at least one court has implicitly reached the opposite conclusion. See *United States v. Coleman*, 2008 WL 495323 at *1 (E.D. Mich. Feb. 20, 2008).

USABook > Electronic Surveillance > Tracking Devices Manual > **Part IV.**
prev | help | download

Part IV:

Internet Protocol (IP) Traceback

- A. Background
 - 1. IP Addresses
 - 2. Regional Internet Registries
- B. Practical Applications

Prosecutors and agents know from experience that a pen register/trap and trace on the telephone of a fugitive's family member (or close friend or romantic interest) can often reveal the fugitive's whereabouts. Having identified a second number in frequent contact with the family member, agents can readily determine the location of that second telephone, especially if it is a landline.

Sometimes overlooked, however, is the fact that this same technique can be used with respect to a fugitive's contacts with online resources. Every time a fugitive logs into his Yahoo! webmail account, Facebook page, or other Internet resource, he reveals information that can be traced to a physical location. This chapter provides a short overview of that process.

A. Background

1. IP Addresses

Just as a telephone needs to be assigned a unique number in order to receive calls from other telephones, every Internet-connected device must be associated with an identifier that uniquely distinguishes it from other Internet computers.[FN1] That universal identifier is known as an **Internet Protocol address**, or **IP address**. IP addresses are by convention written in the form *num1.num2.num3.num4*, where each number lies in the range 0-255—for example, 198.7.0.2.

A conventional end-user computer, such as a laptop with a modem or networking jack, does not "come with" a built-in IP address. (This is no different from a landline phone, which has no pre-assigned phone number when purchased.) Instead, IP addresses are assigned by the operator of the local network—such as a business, university, or Internet service provider—on an as-needed basis whenever the computer is attached to the network.

In almost all cases involving consumer end-users, *i.e.*, ISP customers, an IP address is **dynamically assigned**. Simply put, this means that the computer is not assigned a fixed, predetermined IP address, but rather whatever IP address is available from the host network.

The duration of the assignment typically varies depending on the type of connection. For a user connecting to his ISP via dial-up, the assignment lasts only for the length of the dial-up session; if the user disconnects and immediately initiates a new dial-up connection, his computer will almost always be assigned a different (if similar-looking) IP address for the second session. By contrast, a home user on a broadband connection (DSL, cable, FIOS, etc.) receives an IP address when she first connects her equipment (such as a DSL modem) to the network, and may retain that same IP address[FN2] for weeks or months at a time.

Regardless of the type of connection, the network operator (such as an ISP) typically creates a record of each such assignment. These records are often retained for several months, although practices vary across the industry owing to the absence of any legal retention requirement.

2. Regional Internet Registries

When a phone company wishes to offer service in a given area code, it cannot simply pick which numbers to give its new customers. Instead, it must apply to a central authority to have a currently unused block of numbers—e.g., the 10,000 telephone numbers in the range (202) 259-0000 through (202) 259- 9999—reserved for its exclusive use.

The Internet Protocol "numeric space" is managed in a similar fashion. When ISPs and other network operators assign IP addresses to devices on their networks, they are not free to randomly choose any of the approximately 4.3 billion possible IPv4 addresses. Rather, each operator must first apply to a central authority to have a specific range of available IP addresses allocated for its exclusive use. A large service provider might have several hundred thousand or more IP addresses allocated to it (such as the range 67.100.0.0 to 67.103.255.255—covering 262,144 addresses—currently allocated to DSL service provider Covad).

Instead of a single central authority for IP address allocation, there are five so-called **Regional Internet Registries (RIRs)** performing this function for different geographic regions. The RIR for North America is the American Registry for Internet Numbers (arin.net). Others are RIPE for Europe and portions of Asia (ripe.net); AfrINIC for Africa (afrinic.net); APNIC for the Asia/Pacific region (apnic.net); and LACNIC for Latin America and the Caribbean (lacnic.net). Each RIR maintains a publicly accessible list of IP range allocations.

B. Practical Applications

Suppose you want to locate Fay, who is known to have a Google Gmail account she uses regularly. When Fay logs into her Gmail account, the Gmail server can under normal circumstances observe the IP address of the computer Fay is using.[FN3] That information can be obtained either prospectively (via a trap and trace order[FN4] served on Gmail) or for past periods (via a subpoena or court order under 18 U.S.C. § 2703(d)).

Having determined that Fay was using a given IP address at a given date and time, the next step is to relate it to a physical location. There are two ways to begin this process.

First, an IP address will often be associated with a corresponding **fully qualified domain name**. For instance, IP address 67.101.56.1 corresponds to the name "h-67-101-56-1.mclnva23.dynamic.covad.net". (This type of query, referred to as a **reverse lookup**, may be performed using any of numerous network utilities, including the web- accessible interface at <http://centralops.net>.) In many cases the domain name will contain a rough indication of geographical location—here, an abbreviation for McLean, Virginia. More importantly, it indicates the name of the network operator—here, covad.net—which will have more reliable and precise information about the physical location associated with the IP address.

Significantly, reverse lookup queries will often be unsuccessful owing to network configuration issues beyond the scope of this treatise. Thus, a second type of lookup—**IP whois**, or **IP block lookup**—is almost always more reliable and valuable. As the name implies, an IP block lookup reveals the name of the network operator to whom was allocated the block of contiguous IP addresses containing the specified IP address. (These queries can be run using <http://centralops.net> or the "whois" search tool at arin.net or other applicable RIR.)

As mentioned above, the block containing IP address 67.101.56.1—that is, the range 67.100.0.0 to 67.103.255.255—is allocated to Covad. Given a specific date, time, and time zone[FN5] for that IP address, Covad could authoritatively identify the corresponding service address of that DSL user.[FN6] Notably, that address might not be in the same jurisdiction suggested by the less accurate reverse lookup results—for example, in Washington, DC and not McLean, Virginia.

FN 1. As discussed below, "unique" is not strictly accurate in every case.

FN 2. In such situations, only the user's DSL modem (or other router) receives its own IP address from the ISP, even if there are several computers sharing that connection (such as via a wireless access point). To the outside world, all the computers in that household will appear to have the same IP address. Fortunately, in the vast majority of cases this has no practical impact on the ability to determine the physical location of the user of a given IP address.

FN 3. Although it is possible to "spoof" the return IP address on data packets sent from a computer, doing so prevents the computer receiving the data from successfully sending responses back to the spoofing computer. As a result, it is not possible even to log into Gmail while spoofing one's IP, let alone read one's email over the web.

However, a user can successfully obscure his or her IP address by using a **proxy service**—that is, a computer configured to act as a middleman between the user's computer and the sites visited by the user. Under this arrangement, a server at the visited site (such as Gmail) will observe only the IP address of the proxy.

FN 4. See the Appendix for a model trap and trace application and order.

FN 5. Specifying a time zone is crucial. A Gmail login at 4:35 p.m. local time (Pacific) from a DC-area user would correspond to 7:35 p.m. Eastern time in the dynamic assignment logs of the user's ISP.

FN 6. Of course, ECPA requires either a subpoena or court order (under § 2703(c)) or a relevant exception permitting voluntary disclosure (§ 2702(c)) before a service provider may disclose such customer information.

USABook > Electronic Surveillance > Tracking Devices Manual > **Forms Appendix**

Forms Appendix

Forms for Part I.
(Obtaining Location
Information from Wireless
Carriers)

Form I-1. Rule 41 affidavit & order for prospective E-911 phone location

Form I-2. T-III inserts for prospective E-911 phone location

Form I-3. Prospective cell-site application and order (hybrid authority)

Form I-4. Historical cell site

Form I-5. Tower dump application & order

Form I-6. Prospective sat. phone location app. & order (hybrid authority)

Forms for Part II.
(Mobile Tracking Devices)

Form II-1. Tracking device affidavit and order

Forms for Part III.
(Telematics Providers
(OnStar, etc.)

Form III-1. OnStar model affidavit & order

Forms for Part IV.
(Internet Protocol (IP)
Traceback)

Form IV-1. Model form for IP trap and trace on a Web-based account

The attached forms are for use in obtaining relatively precise location information concerning a wireless phone, with assistance from the carrier as needed. They do not refer to "GPS" as that term is technically inaccurate in describing the location-finding capabilities of some wireless carriers. ***Do not use these forms if you want only cell tower/sector records*** (sometimes referred to as "cell-site data" or "tower/face information") unless your local judges refuse to grant "hybrid" 3123/2703(d) orders for this less precise class of information.

Note that these forms do not invoke 18 USC § 3117 (the tracking device statute) nor the Rule 41 provisions concerning "tracking devices." The Department's position is that a cell phone knowingly possessed by a user is not a "tracking device" within the meaning of that term as defined in section 3117. However, because a reviewing court might instead conclude that a user's own phone falls within the definition, as a precaution these forms include space in the return for indicating when the location-finding activity is first initiated and for what period.

Important considerations in using these forms include

- where to apply: Rule 41(b)(2) states that a warrant may issue for "a person or property outside the district if [it] is located within the district when the warrant is issued." However, the Criminal Division believes that 18 U.S.C. § 2703(c)(1)(A), which permits the compulsion of records and other information from service providers outside the district, overrides the limitations in Rule 41. Under this approach, prosecutors may obtain a warrant for prospective geolocation information from a "court of competent jurisdiction" (as defined at 18 U.S.C. § 2711(3)), including a court with jurisdiction over the offense under investigation, without regard to the location of the target phone.
- delay of notice: 18 USC § 3103a(b)(3) and Rule 41(f)(3) permit notice to be delayed up to 30 days initially.

However, AUSAs in the Ninth Circuit should note *United States v. Freitas*, 800 F.2d 1451, 1456 (9th Cir. 1986), which holds that absent unusual circumstances, the Fourth Amendment forbids a delay of more than 7 days (subject to extension upon application to the court) in notifying the owner of premises searched pursuant to a warrant. This holding has been expressly rejected elsewhere – see *United States v. Pangburn*, 983 F.2d 449, 455 (2d Cir. 1993) – and is manifestly incompatible with the provision in Title III permitting delay of notice of an interception order for up to 90 days. See 18 U.S.C. § 2518(8)(d), the constitutionality of which was upheld in *United States v. Cafaro*, 473 F.2d 489, 501 & n.9 (3d Cir. 1973) (citing numerous cases reaching the same conclusion).

- persons to be notified: OEO recommends giving notice to the person(s) who actually used the target phone, and not merely to the registered owner (if different)

Applicants with additional questions are encouraged to contact the author of this form (Mark Eckenwiler, Associate Director, Office of Enforcement Operations, (b) (6), (b) (7)(C) or mark.eckenwiler@usdoj.gov).

Revised 2-14-11; current version available at
<http://dojnet.doj.gov/usao/eousa/ole/usabook/cell/01cell01.wpd>

UNITED STATES DISTRICT COURT
DISTRICT OF

IN THE MATTER OF THE APPLICATION
OF THE UNITED STATES OF AMERICA
FOR AUTHORIZATION TO OBTAIN LOCATION
DATA CONCERNING A CELLULAR TELEPHONE
ASSIGNED CALL NUMBER (xxx) xxx-xxxx,
WITH [INTERNATIONAL MOBILE SUBSCRIBER
IDENTITY / ELECTRONIC SERIAL NUMBER]
XXXXXXXXXXXXXXXXXXXX

UNDER SEAL

AFFIDAVIT IN SUPPORT
OF APPLICATION

STATE OF _____)
COUNTY OF _____ : ss.:
_____ DISTRICT OF _____)

_____, a Special Agent with the _____, being duly
sworn, deposes and states:

INTRODUCTION

1. I am a "federal law enforcement officer" within
the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C),
that is, a government agent engaged in enforcing the criminal
laws and duly authorized by the Attorney General to request a
search warrant. I have been a _____ agent since _____. I have
participated in investigations of _____ and, among other
things, have conducted or participated in surveillances, the
execution of search warrants, debriefings of informants and
reviews of taped conversations. Through my training, education
and experience, I have become familiar with the manner in which

2. I submit this affidavit in support of an
application for a warrant pursuant to Federal Rule of Criminal
Procedure 41 and 18 U.S.C. 2703(c)(1)(A), authorizing agents of

the ____ to ascertain the physical location of the cellular telephone assigned call number (xxx) xxx-xxxx, with [International Mobile Subscriber Identity /Electronic Serial Number] xxxxxxxxxxxxxxxx, subscribed to in the name _____ at ____ [address] ____, with service provided by [carrier] (the "TARGET CELLPHONE"), including but not limited to E-911 Phase II data (or other precise location information) concerning the TARGET CELLPHONE (the "Requested Information"),¹ for a period of thirty (30) days.

3. I have personally participated in the investigation set forth below. I am familiar with the facts and circumstances of the investigation through my personal participation; from discussions with other agents of the ____ and other law enforcement; from my discussions with witnesses involved in the investigation; and from my review of records and reports relating to the investigation. Unless otherwise noted, wherever in this affidavit I assert that a statement was made, the information was provided by another ____ agent, law

¹Such information shall, where other information is unavailable, include records reflecting the tower and antenna face ("cell site") used by the TARGET CELLPHONE at the start and end of any call. In requesting cell site information, the Government does not concede that such cell site records - routinely retained by wireless carriers as business records - may only be obtained via a warrant issued on probable cause. See In re Application, 460 F. Supp. 2d 448 (S.D.N.Y. 2006) (authorizing prospective acquisition of cell-site records under combined authority of 18 U.S.C. 2703(d) & 3121 et seq.).

enforcement officer or witness who may have had either direct or hearsay knowledge of that statement and to whom I or others have spoken or whose reports I have read and reviewed. Such statements are among many statements made by others and are stated in substance and in part unless otherwise indicated. Since this affidavit is being submitted for the limited purpose of securing an order authorizing the acquisition of the Requested Information, I have not included details of every aspect of the investigation. Facts not set forth herein, or in the attached exhibits, are not being relied on in reaching my conclusion that the requested warrant should be issued. Nor do I request that this Court rely on any facts not set forth herein in reviewing this application.

4. Probable cause exists to believe that the Requested Information will constitute or lead to evidence of offenses involving _____, in violation of _____ (the "TARGET OFFENSES"), as well as the identification of individuals who are engaged in the commission of these offenses.

5. For the reasons set out in this affidavit, there is probable cause to believe that the TARGET OFFENSES have been committed, are being committed, and will continue to be committed by _____ and others unknown. [Further, there is probable cause to believe that _____ is using the TARGET CELLPHONE to commit the TARGET OFFENSES.]

Background of the Investigation

6. This application is submitted in connection with a _____ investigation of _____.

7. Based on information obtained from _____, _____ regularly carries the TARGET CELLPHONE [and uses it to conduct illegal activities].

8. The investigation, through, among other things, the use of confidential sources and _____, has revealed, among other things, that _____ and others are engaged in _____.

[Set forth facts tying target cellphone to illegal activities.]

AUTHORIZATION REQUEST

9. Based on the foregoing, there is probable cause to believe that the Requested Information will lead to evidence regarding the activities described above. The Requested Information is necessary to determine the location of _____ so that [e.g., law enforcement agents can conduct physical surveillance of _____ in connection with this expected transaction].

10. WHEREFORE, pursuant to Federal Rule of Criminal Procedure 41 and 18 U.S.C. 2703(c)(1)(A), it is requested that the Court issue a warrant and Order authorizing agents of _____ to

obtain the Requested Information for a period of thirty (30) days.

11. IT IS FURTHER REQUESTED that the Court direct [carrier] to assist agents of the _____ by providing all information, facilities and technical assistance needed to ascertain the Requested Information, and further direct [carrier], the service provider for the TARGET CELLPHONE, to initiate a signal to determine the location of the TARGET CELLPHONE on the service provider's network or with such other reference points as may be reasonably available and at such intervals and times as directed by the law enforcement agent serving the proposed warrant, and to furnish the technical assistance necessary to accomplish the acquisition unobtrusively and with a minimum of interference with such services as that provider accords the user(s) of the TARGET CELLPHONE, for a period of thirty (30) days. Reasonable expenses incurred pursuant to this activity will be processed for payment by the _____.

12. IT IS FURTHER REQUESTED that the Court authorize execution of the warrant at any time of day or night, owing to the potential need to locate the TARGET CELLPHONE outside of daytime hours.

13. IT IS FURTHER REQUESTED that the warrant and this Affirmation, as it reveals an ongoing investigation, be sealed

until further order of the Court in order to avoid premature disclosure of the investigation, guard against flight, and better ensure the safety of agents and others, except that working copies may be served on Special Agents and other investigative and law enforcement officers of the ____, federally deputized state and local law enforcement officers, and other government and contract personnel acting under the supervision of such investigative or law enforcement officers, and [carrier] as necessary to effectuate the Court's Order.

14. IT IS FURTHER REQUESTED that, pursuant to 18 U.S.C. 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), the Court authorize notice to be delayed for a period of [INSERT NUMBER NO GREATER THAN 30; SEE ALSO COVER SHEET] days after the termination of the monitoring period authorized by the warrant or any extensions thereof, because there is reasonable cause to believe that providing immediate notification would seriously jeopardize the investigation.

Special Agent

Sworn to before me this
___ day of ___ 201__

UNITED STATES MAGISTRATE JUDGE

DISTRICT OF _____

UNITED STATES DISTRICT COURT
DISTRICT OF

IN THE MATTER OF THE APPLICATION
OF THE UNITED STATES OF AMERICA
FOR AUTHORIZATION TO OBTAIN LOCATION
DATA CONCERNING A CELLULAR TELEPHONE
ASSIGNED CALL NUMBER (xxx) xxx-xxxx,
WITH [INTERNATIONAL MOBILE SUBSCRIBER
IDENTITY / ELECTRONIC SERIAL NUMBER]
XXXXXXXXXXXXXXXXXXXX

SEALED WARRANT

Application having been made by the United States for a warrant pursuant to Federal Rule of Criminal Procedure 41 and 18 U.S.C. 2703(c) (1) (A), authorizing agents of the ___ to ascertain the physical location of the cellular telephone assigned call number (xxx) xxx-xxxx, with [International Mobile Subscriber Identity / Electronic Serial Number] xxxxxxxxxxxxxxxx, subscribed to in the name _____ at ___ [address] ___, with service provided by [carrier] (the "TARGET CELLPHONE"), including but not limited to E-911 Phase II data (or other precise location information) concerning the TARGET CELLPHONE (the "Requested Information"),² for a period of thirty (30) days;

The Court finds that there is probable cause to believe that the Requested Information will constitute or lead to evidence of violations of Title __, United States Code, Sections ___ and ___,

²Such information shall, where other information is unavailable, include records reflecting the tower and antenna face ("cell site") used by the TARGET CELLPHONE at the start and end of any call.

among other offenses, as well as to the identification of individuals who are engaged in the commission of these offenses.

~~IT IS HEREBY ORDERED~~ pursuant to Federal Rule of Criminal Procedure 41 and 18 U.S.C. 2703(c)(1)(A) that agents of _____, beginning at any time within ten (10) days of the date of this warrant and for a period not to exceed 30 days, may obtain the Requested Information concerning the TARGET CELLPHONE, with said authority to extend to any time of the day or night as required, including when the TARGET CELLPHONE leaves the _____ District of _____; all of said authority being expressly limited to ascertaining the physical location of the TARGET CELLPHONE and expressly excluding the contents of any communications conducted by the user(s) of the TARGET CELLPHONE.

It is further ORDERED that [carrier], the service provider for the TARGET CELLPHONE, assist agents of the _____ by providing all information, facilities and technical assistance needed to ascertain the Requested Information, including by initiating a signal to determine the location of the subject's mobile device on [carrier's] network or with such other reference points as may be reasonably available and at such intervals and times as directed by the law enforcement agent serving the warrant, and furnish the technical assistance necessary to accomplish the acquisition unobtrusively and with a minimum of interference with such services as [carrier] accords the user(s) of the TARGET

CELLPHONE.

It is further ORDERED that the ____ compensate [carrier] for reasonable expenses incurred in complying with any such request.

It is further ORDERED that this warrant and the accompanying Affidavit submitted in support thereof, as they reveal an ongoing investigation, be sealed until further order of the Court in order to avoid premature disclosure of the investigation, guard against flight, and better ensure the safety of agents and others, except that copies of the warrant in full or redacted form may be maintained by the United States Attorney's Office, and may be served on Special Agents and other investigative and law enforcement officers of the ____, federally deputized state and local law enforcement officers, and other government and contract personnel acting under the supervision of such investigative or law enforcement officers, and [carrier] as necessary to effectuate the Court's Order and warrant.

It is further ORDERED that this warrant be returned to the issuing judicial officer within 10 days after the termination of the monitoring period authorized by the warrant.

It is further ORDERED that, pursuant to 18 U.S.C. 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), service of

notice may be delayed for a period of [INSERT NUMBER NO GREATER THAN 30; SEE ALSO COVER SHEET] days after the termination of the monitoring period authorized by the warrant or any extension thereof, because there is reasonable cause to believe that providing immediate notification would seriously jeopardize the investigation.

It is further ORDERED that [carrier], its affiliates, officers, employees, and agents not disclose this warrant or the underlying investigation, until notice is given as provided above.

It is further ORDERED that this warrant apply to any changed cellular telephone number subsequently assigned to the Target Telephone within the period of this warrant.

Dated: _____ day of _____ 201__

Time: _____

UNITED STATES MAGISTRATE JUDGE

DISTRICT OF _____

WARRANT ON WRITTEN AFFIDAVIT FOR CELL PHONE LOCATION DATA

<p><i>United States District Court</i></p>	<p>DISTRICT</p> <p>_____ District of _____</p>	
<p>UNITED STATES OF AMERICA</p> <p>v.</p> <p>PREMISES KNOWN AND DESCRIBED AS A CELLULAR TELEPHONE ASSIGNED CALL NUMBER (xxx) xxx-xxxx, WITH [INTERNATIONAL MOBILE SUBSCRIBER IDENTITY / ELECTRONIC SERIAL NUMBER] xxxxxxxxxxxxxxxxxxxx</p>	<p>DOCKET NO.</p>	<p>MAGISTRATE'S CASE NO.</p>
	<p>To:</p> <p>ANY AUTHORIZED FEDERAL AGENT</p>	
<p>Affidavit having been made before me by the below-named affiant to obtain precise location information concerning the following cell phones (the "Premises"):</p> <p>A CELLULAR TELEPHONE ASSIGNED CALL NUMBER (xxx) xxx-xxxx, WITH [INTERNATIONAL MOBILE SUBSCRIBER IDENTITY / ELECTRONIC SERIAL NUMBER] xxxxxxxxxxxxxxxxxxxx</p> <p>and as I am satisfied that there is probable cause for the acquisition of precise location information concerning the Premises,</p> <p>YOU ARE HEREBY COMMANDED to acquire precise location data concerning the Premises named above for a period of thirty (30) days starting within ten (10) calendar days of the date of this warrant, during any time of day; to return this warrant to the <u>U.S. Magistrate Judge</u> designated in this warrant within ten (10) calendar days after the monitoring period authorized by the warrant has ended; and pursuant to 18 U.S.C. § 3103a(b)(3) (authorizing delayed notification), to serve notice within [INSERT NUMBER NO GREATER THAN 30; SEE ALSO COVER SHEET] after the monitoring period authorized by the warrant has ended.</p>		
<p>NAME OF AFFIANT</p> <p>Special Agent _____</p>	<p>SIGNATURE OF JUDGE OR U.S. MAGISTRATE</p>	<p>DATE/TIME ISSUED</p>

RETURN

DATE AND TIME ACQUISITION OF LOCATION DATA FIRST INITIATED AND PERIOD DURING WHICH IT WAS ACQUIRED:

CERTIFICATION

I swear that this information contained on this return is true and accurate:

Subscribed, sworn to, and returned before me this date.

Federal Judge or U.S. Magistrate

Date

Title III Inserts for Seeking E-911/Geolocation Data

The form language on the following pages is intended for use in requesting, in conjunction with a Title III application, E-911 Phase II (precise location) information concerning the target wireless telephone. Use of the separate warrant form at the end is optional but recommended, as it simplifies the process of making the return to the court (as discussed in Part I.B.1 of the foregoing manual on location technologies).

Questions about this form or requests for advice may be directed to OEO Associate Director Mark Eckenwiler at (b) (6), (b) (7)(C) or mark.eckenwiler@usdoj.gov.

Revised 8-19-09

Current version available at <http://dojnet.doj.gov/usao/eousa/ole/usabook/cell/01cell02.wpd>

Inserts to Affidavit

In addition, there is probable cause to believe that the location of the TARGET PHONE at times determined by investigators will constitute or lead to evidence of the SUBJECT OFFENSES. [Set out facts supporting the claim that location information will be relevant. The probable cause supporting the wiretap application will in most cases also justify acquisition of location info; however, it is nevertheless important to provide a separate – if brief – justification for also obtaining location information.]

Inserts to Application

IT IS FURTHER REQUESTED, pursuant to Federal Rule of Criminal Procedure 41, that the Court issue an Order authorizing agents of the [AGENCY] to ascertain the physical location of the TARGET PHONE, including but not limited to E-911 Phase II data or other precise location information concerning the TARGET PHONE (the "Requested Location Information"),¹ during the authorized period of interception. As explained in more detail in the Affidavit, there is probable cause to believe that the location of the TARGET PHONE during that period will constitute or lead to evidence of the SUBJECT OFFENSES.

IT IS FURTHER REQUESTED that the Court direct [CARRIER] to disclose the Requested Location Information concerning the TARGET PHONE during the authorized period of interception, and to initiate a signal to determine the location of the TARGET PHONE on the service provider's network or with such other reference points as may be reasonably available and at such intervals and times as directed by the law enforcement agent serving the proposed order, and to furnish the information, facilities and technical assistance necessary to accomplish the acquisition unobtrusively and with a minimum of interference with such services as that provider accords the user(s) of the TARGET PHONE, at any time of day or night, owing to the potential need to locate the TARGET PHONE outside of daytime hours.

IT IS FURTHER REQUESTED, pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), that the Court authorize delay of notice of the acquisition of the Requested Location Information until such time as the inventory required under 18 U.S.C. § 2518(8)(d) is served..

¹Such information shall, where other information is unavailable, include records reflecting the tower and antenna face ("cell site") used by the TARGET PHONE at the start and end of any call. In requesting cell site information, the Government does not concede that such cell site records – routinely retained by wireless carriers as business records – may only be obtained via a warrant issued on probable cause. *See In re Application*, 460 F. Supp. 2d 448 (S.D.N.Y. 2006) (authorizing prospective acquisition of cell-site records under combined authority of 18 U.S.C. §§ 2703(d) & 3121 et seq.).

Inserts to Order

IT IS FURTHER ORDERED, pursuant to Rule 41 of the Federal Rules of Criminal Procedure, that agents of the [AGENCY] are authorized to ascertain the physical location of the TARGET PHONE, including but not limited to E-911 Phase II data or other precise location information concerning the TARGET PHONE (the "Requested Location Information"),² during the authorized period of interception.

IT IS FURTHER ORDERED that [CARRIER] shall disclose the Requested Location Information concerning the TARGET PHONE during the authorized period of interception, and shall initiate a signal to determine the location of the TARGET PHONE on the service provider's network or with such other reference points as may be reasonably available and at such intervals and times as directed by the law enforcement agent serving the proposed order, and shall furnish the information, facilities and technical assistance necessary to accomplish the acquisition unobtrusively and with a minimum of interference with such services as that provider accords the user(s) of the TARGET PHONE, at any time of day or night, owing to the potential need to locate the TARGET PHONE outside of daytime hours.

IT IS FURTHER ORDERED that the furnishing of said information, facilities, and technical assistance by [CARRIER] shall terminate thirty days measured from the earlier of the day on which the investigative or law enforcement officers begin to conduct the interception of wire communications, pursuant to this Order or ten days from the date of the order is entered, unless otherwise ordered by this Court.

IT IS FURTHER ORDERED that the furnishing of such information, facilities and assistance by [CARRIER] shall be compensated for by the United States at the prevailing rate.

IT IS FURTHER ORDERED that the warrant for the Requested Location Information be returned to the issuing judicial officer within 10 days after the termination of the authorized period of interception .

IT IS FURTHER ORDERED, pursuant to 18 U.S.C. 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), that service of notice of the acquisition of the Requested Location Information may be delayed until such time as the inventory required under 18 U.S.C. § 2518(8)(d) is served..

²Such information shall, where other information is unavailable, include records reflecting the tower and antenna face ("cell site") used by the TARGET PHONE at the start and end of any call.

Inserts to Provider Order

IT IS FURTHER ORDERED, pursuant to Rule 41 of the Federal Rules of Criminal Procedure, that agents of the [AGENCY] are authorized to ascertain the physical location of the TARGET PHONE, including but not limited to E-911 Phase II data or other precise location information concerning the TARGET PHONE (the "Requested Location Information"),³ during the authorized period of interception.

IT IS FURTHER ORDERED that [CARRIER] shall disclose the Requested Location Information concerning the TARGET PHONE during the authorized period of interception, and shall initiate a signal to determine the location of the TARGET PHONE on the service provider's network or with such other reference points as may be reasonably available and at such intervals and times as directed by the law enforcement agent serving the proposed order, and shall furnish the information, facilities and technical assistance necessary to accomplish the acquisition unobtrusively and with a minimum of interference with such services as that provider accords the user(s) of the TARGET PHONE, at any time of day or night, owing to the potential need to locate the TARGET PHONE outside of daytime hours.

IT IS FURTHER ORDERED that the furnishing of said information, facilities, and technical assistance by [CARRIER] shall terminate thirty days measured from the earlier of the day on which the investigative or law enforcement officers begin to conduct the interception of wire communications, pursuant to this Order or ten days from the date of the order is entered, unless otherwise ordered by this Court.

IT IS FURTHER ORDERED that the furnishing of such information, facilities and assistance by [CARRIER] shall be compensated for by the United States at the prevailing rate.

³Such information shall, where other information is unavailable, include records reflecting the tower and antenna face ("cell site") used by the TARGET PHONE at the start and end of any call.

WARRANT ON WRITTEN AFFIDAVIT FOR CELL PHONE LOCATION DATA

<p align="center"><i>United States District Court</i></p>	<p align="center">DISTRICT</p> <p align="center">_____ District of _____</p>	
	<p align="center">UNITED STATES OF AMERICA</p> <p align="center">v.</p>	<p>DOCKET NO.</p>
<p>PREMISES KNOWN AND DESCRIBED AS A CELLULAR TELEPHONE ASSIGNED CALL NUMBER (xxx) xxx-xxxx, WITH [INTERNATIONAL MOBILE SUBSCRIBER IDENTITY / ELECTRONIC SERIAL NUMBER] xxxxxxxxxxxxxxxxxxxx</p>	<p>To: ANY AUTHORIZED FEDERAL AGENT</p>	
<p>Affidavit having been made before me by the below-named affiant to obtain precise location information concerning the following cell phones (the "Premises"):</p> <p>A CELLULAR TELEPHONE ASSIGNED CALL NUMBER (xxx) xxx-xxxx, WITH [INTERNATIONAL MOBILE SUBSCRIBER IDENTITY / ELECTRONIC SERIAL NUMBER] xxxxxxxxxxxxxxxxxxxx</p> <p>and as I am satisfied that there is good cause for the acquisition of precise location information concerning the Premises,</p> <p>YOU ARE HEREBY COMMANDED to acquire precise location data concerning the Premises named above for a period of thirty (30) days starting within ten (10) calendar days of the date of this order, during any time of day; to return this warrant to the <u>U.S. Magistrate Judge</u> designated in this warrant within ten (10) calendar days after the execution of the warrant has ended; and pursuant to 18 U.S.C. § 3103a(b)(3) authorizing delayed notification, to serve notice concurrent with the inventory (under 18 U.S.C. § 2518(8)(d)) pertaining to the accompanying order authorizing interception of communications.</p>		
<p>NAME OF AFFIANT</p> <p>Special Agent _____</p>	<p>SIGNATURE OF JUDGE OR U.S. MAGISTRATE</p>	<p>DATE/TIME ISSUED</p>

RETURN

CRM-0003

DATE AND TIME ACQUISITION OF LOCATION DATA FIRST INITIATED AND PERIOD DURING WHICH IT WAS ACQUIRED:

CERTIFICATION

I swear that this information contained on this return is true and accurate:

Subscribed, sworn to, and returned before me this date.

Federal Judge or U.S. Magistrate

Date

Prospective Cell-Site Location Information

The attached forms are intended for use in requesting future cell-site (tower/sector) location information concerning a wireless telephone.

Questions or requests for advice may be directed to OEO Associate Director Mark Eckenwiler at (b) (6), (b) (7)(C) or mark.eckenwiler@usdoj.gov.

Revised 8-19-09

Current version available at <http://dojnet.doj.gov/usao/eousa/ole/usabook/cell/01cell03.wpd>

IN THE UNITED STATES DISTRICT COURT

FOR THE ___ DISTRICT OF ___

IN THE MATTER OF THE APPLICATION)
OF THE UNITED STATES OF AMERICA)
FOR AN ORDER AUTHORIZING THE)
INSTALLATION AND USE OF A PEN)
REGISTER AND TRAP AND TRACE)
DEVICE AND ACQUISITION OF)
CELL SITE INFORMATION FOR)
TELEPHONE NUMBER _____)
[WITH ESN/IMSI NUMBER _____])

UNDER SEAL

NO. _____

APPLICATION

_____, an attorney of the United States Department of Justice, hereby applies to the Court pursuant to 18 U.S.C. §§ 3122, 3123, and 2703(d) for an Order 1) authorizing the installation and use of a pen register and trap and trace device ("Pen/Trap") on the cellular telephone bearing number _____ and ESN/IMSI _____ (the "Target Telephone") and 2) authorizing acquisition of information reflecting the location of cellular towers (cell site and sector/face) related to the use of the Target Telephone ("cell-site information"). In support of this application, Applicant states the following:

1. Applicant is an "attorney for the Government" as defined in Fed. R. Crim. P. 1, and therefore may apply, pursuant to 18 U.S.C. §§ 2703(d) and 3122, for an Order authorizing the installation and use of a Pen/Trap and acquisition of cell-site information.

2. Pursuant to 18 U.S.C. § 3123(a)(1), upon an application made under 18 U.S.C. § 3122(a)(1) a court "shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device anywhere within the United States, if the court finds that the attorney

for the Government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.”

3. Pursuant to 18 U.S.C. § 2703(d), a court may order an electronic communication service to disclose non-content information about a customer or subscriber if the government “offers specific and articulable facts showing that there are reasonable grounds to believe that the . . . records or other information sought are . . . relevant and material to an ongoing criminal investigation.”

4. Cellular telephone companies routinely create and maintain, in the regular course of their business, records of information concerning their customers’ usage. These records typically include for each communication a customer makes or receives (1) the date and time of the communication ; (2) the telephone numbers involved; (3) the cell tower to which the customer connected at the beginning of the communication ; (4) the cell tower to which the customer was connected at the end of the communication ; and (5) the duration of the communication. The records may also, but do not always, specify a particular sector of a cell tower used to transmit a communication.¹ Cell-site information is useful to law enforcement because of the limited information it provides about the general location of a cell phone when a communication is made.

As one court has explained:

The information does not provide a “virtual map” of the user’s location. The information does not pinpoint a user’s location within a building. Instead, it only identifies a nearby cell tower and, for some carriers, a 120-degree face of that tower. These towers can be up to 10 or more miles apart in rural areas and may be up to a half-mile or more apart even in urban areas.

¹ Cell towers are often divided into three 120° sectors, with separate antennas for each of the three sectors. To the extent this information does exist in a particular instance, it does not provide precise information regarding the location of the cell phone at the time of the communication, but instead shows only in which of the three 120°, pie-shaped sectors the phone was probably located.

In re Application of United States for an Order for Disclosure of Telecommunications Records, 405 F. Supp. 2d 435, 449 (S.D.N.Y. 2005) (citation omitted).

5. By this application, the government seeks an order authorizing (1) the installation and use of a Pen/Trap on the Target Telephone and (2) the acquisition of cell-site information related to the use of the Target Telephone. The requested information does not include GPS data or other E-911 Phase II location information.

6. Applicant certifies that the [AGENCY NAME] (the "Investigative Agency") is conducting an ongoing criminal investigation of [TARGET NAMES], and others both known and as yet unknown, in connection with possible violations of __ U.S.C. § _____. It is believed that one or more subjects of the investigation possess and are using the Target Telephone, which is subscribed to by [SUBSCRIBER NAME], [SUBSCRIBER ADDRESS], with service provided by [SERVICE PROVIDER NAME].

7. Further, as required under 18 U.S.C. § 2703(d), Applicant offers the following specific and articulable facts showing that there are reasonable grounds to believe that the cell-site information sought is relevant and material to this ongoing criminal investigation.

8. **[Set out specific facts explaining the relevance of the requested cell-site information. It is not necessary to show that the communications themselves are expected to be in furtherance of the offenses under investigation; for example, location records for a non-criminal call may nevertheless place a target in the general vicinity of a narcotics delivery or other criminal event.]**

#. Because the assistance of [SERVICE PROVIDER NAME] will be necessary to accomplish the objectives of the requested order, Applicant further requests that the Order direct that,

upon service of the order upon it, [SERVICE PROVIDER NAME] furnish information, facilities, and technical assistance necessary to accomplish the installation of the Pen/Trap, including installation and operation of the devices unobtrusively and with a minimum of disruption of normal service. [SERVICE PROVIDER NAME] shall be compensated by Investigative Agency for reasonable expenses incurred in providing such facilities and assistance in furtherance of the Order.

#. Notification to the subscriber or customer or to any other unauthorized person of the issuance of the anticipated Order (or the existence of the investigation) would seriously jeopardize said investigation. Due to the sensitive nature of this investigation and in order to protect the sources and methods involved in this investigation, it is respectfully requested that, pursuant to 18 U.S.C. § 3123(d), the Application and anticipated Order in this matter be filed under seal, until further order of this Court. For the same reasons, it is also respectfully requested that pursuant to 18 U.S.C. §§ 2705(b) and 3123(d), this Court order [SERVICE PROVIDER NAME] not to disclose the existence of the application, the resulting court order, or the investigation to the listed subscriber for any reason or to any other person, except as required to execute the order, unless or until ordered by this Court.

WHEREFORE, IT IS REQUESTED that this Court enter an ex parte Order for a period of sixty (60) days, commencing upon the date of installation of the Pen/Trap, authorizing the installation and use of a Pen/Trap to collect the dialing, routing, addressing, and signaling information (including date and time) associated with communications to or from the Target Telephone.

IT IS FURTHER REQUESTED that the Order authorize agents of the Investigative Agency to acquire, during the same 60-day period, cell-site information for communications to and from the Target Telephone as well the physical location of the cellular towers(s) identified thereby.

IT IS FURTHER REQUESTED that the Order direct [SERVICE PROVIDER NAME] to furnish agents of the Investigative Agency forthwith all information, facilities, and technical assistance necessary to effectuate the Order unobtrusively and with minimum interference to the services accorded to the user of the Target Telephone.

IT IS FURTHER REQUESTED that this Application and the anticipated Order of this Court be filed under seal, and that the Court direct [SERVICE PROVIDER NAME] not to disclose to any person the existence of this Application, the resulting Order, or the investigation for any reason, except as required to execute the Order, unless or until ordered otherwise by this Court.

IT IS FURTHER REQUESTED that the Court's Order apply to any changed cellular telephone number subsequently assigned to the Target Telephone within the period of the Order.

Applicant declares and certifies, under penalty of perjury, that to the best of Applicant's knowledge and belief, the foregoing is true and correct.

[NAME]
Assistant U.S. Attorney

SUBSCRIBED and SWORN to before me this _____ day of _____, 200__.

[NAME]
UNITED STATES MAGISTRATE JUDGE

IN THE UNITED STATES DISTRICT COURT

FOR THE ___ DISTRICT OF ___

IN THE MATTER OF THE APPLICATION)
OF THE UNITED STATES OF AMERICA)
FOR AN ORDER AUTHORIZING THE)
INSTALLATION AND USE OF A PEN)
REGISTER AND TRAP AND TRACE)
DEVICE AND ACQUISITION OF)
CELL-SITE INFORMATION FOR)
TELEPHONE NUMBER _____)
[WITH ESN/IMSI NUMBER _____])

UNDER SEAL

NO. _____

ORDER

This matter having come before the Court pursuant to an Application under 18 U.S.C. §§ 3122, 3123, and 2703(d) by _____, Assistant United States Attorney for the ___ District of ___, which Application requests an Order authorizing the installation and use of a pen register and trap and trace device ("Pen/Trap") on the cellular telephone bearing phone number _____ and ESN/IMSI _____ (the "Target Telephone"), and the acquisition of information reflecting the location of cellular towers (cell site and sector/face) related to the use of the Target Telephone ("cell-site information"), the Court finds:

1. The Applicant has certified that the [AGENCY NAME] (the "Investigative Agency") is conducting an ongoing criminal investigation of [TARGET NAMES], and others both known and as yet unknown, in connection with possible violations of ___ U.S.C. § ___, [OFFENSE];

2. The Applicant has further certified that one or more subjects of the investigation are believed to be using the Target Telephone, subscribed to by [SUBSCRIBER NAME], [SUBSCRIBER ADDRESS], with service provided by [SERVICE PROVIDER NAME]; and

3. The Applicant has offered specific and articulable facts showing that there are reasonable grounds to believe that the requested cell-site information is relevant and material to the ongoing criminal investigation.

IT IS THEREFORE ORDERED, pursuant to 18 U.S.C. § 3123, that agents of the Investigative Agency may, for a period of sixty (60) days commencing upon the date of installation of the Pen/Trap, install and use a Pen/Trap to collect the dialing, routing, addressing, and signaling information (including date and time) associated with communications to or from the Target Telephone.

IT IS FURTHER ORDERED that agents of the Investigative Agency are authorized to acquire, during the same 60-day period, cell-site information for communications to and from the Target Telephone as well the physical location of the cellular towers(s) identified thereby, but not to include GPS data or other E-911 Phase II location information.

IT IS FURTHER ORDERED that [SERVICE PROVIDER NAME] furnish agents of the Investigative Agency forthwith all information, facilities, and technical assistance necessary to effectuate the Order unobtrusively and with minimum interference to the services accorded to the user(s) of the Target Telephone, and that [SERVICE PROVIDER NAME] be compensated by the Investigative Agency for reasonable expenses incurred in providing such facilities and technical assistance.

IT IS FURTHER ORDERED that this Order and the underlying Application be sealed, and that [SERVICE PROVIDER NAME] not disclose to any person the existence of this Order, the underlying Application, or the investigation for any reason, except as required to execute the Order, unless or until ordered otherwise by this Court.

IT IS FURTHER ORDERED that this Order apply to any changed cellular telephone number subsequently assigned to the Target Telephone within the period of this Order.

SIGNED this _____ day of _____, 200_.

[NAME]
UNITED STATES MAGISTRATE JUDGE

Historical Cell-Site Location Information

The attached forms are intended for use in requesting historical cell-site (tower/sector) location information concerning a wireless telephone.

Questions or requests for advice may be directed to OEO Associate Director Mark Eckenwiler at (b) (6), (b) (7)(C) or mark.eckenwiler@usdoj.gov.

Revised 8-19-09

Current version available at <http://dojnet.doj.gov/usao/eousa/ole/usabook/cell/01cell04.wpd>

IN THE UNITED STATES DISTRICT COURT FOR THE
_____ DISTRICT OF _____

IN THE MATTER OF THE APPLICATION)	
OF THE UNITED STATES OF AMERICA)	
FOR AN ORDER PURSUANT TO 18 U.S.C.)	No:
§ 2703(d) DIRECTING [PROVIDER])	
TO PROVIDE HISTORICAL CELL)	
SITE LOCATION RECORDS RELATED)	<u>UNDER SEAL</u>
TO TELEPHONE NUMBER)	
[(XXX) XXX-XXXX])	

APPLICATION FOR COURT ORDER
FOR DISCLOSURE OF HISTORICAL CELL-SITE RECORDS

The United States of America hereby moves this Court pursuant to 18 U.S.C. § 2703(c)-(d) for an order (1) requiring [PROVIDER], an electronic communication service within the meaning of 18 U.S.C. § 2510(15), to disclose to [LAW ENFORCEMENT AGENCY] records reflecting the location of cellular towers (cell site and sector/face) related to the use of a cellular telephone assigned the telephone number (XXX) XXX-XXXX for the period from [DATE 1] to [PRESENT/DATE 2]; (2) precluding the provider of such service from disclosing to the subscriber or customers or to any other unauthorized person this request, any court order issued in connection with this request, the fact of disclosure of such records to [LAW ENFORCEMENT AGENCY] or the existence of this investigation, pursuant to 18 U.S.C. § 2705(b); and (3) sealing the government's application, the court's order, and any related documents.

In support of this application, the undersigned states as follows:

1. The undersigned is an attorney for the government as defined by Rule 1(b) of the Federal Rules of Criminal Procedure and, therefore, pursuant to 18 U.S.C. § 2703(c) may apply

for an order as requested herein.

2. **[LAW ENFORCEMENT AGENCY]** is conducting a criminal investigation involving **[SHORT DESCRIPTION OF CRIMINAL ACTS]** and the investigation continues in connection with possible criminal violations, including, among others, 18 U.S.C. § **[STATUTE]**; that it is believed that a subject[s] of the investigation have used a cellular telephone assigned the telephone number **[(XXX) XXX-XXXX]** listed in the name of **[NAME AND ADDRESS]** during the period **[DATE 1]** to **[PRESENT/DATE 2]**; and that the requested location records for cellular towers (cell site and sector/face) used to make or receive calls on the subject cellular phone are relevant and material to the ongoing criminal investigation.

3. **[Set out specific facts explaining the relevance of the requested location records. It is not necessary to show that the communications themselves were in furtherance of the offenses under investigation; for example, location records for a non-criminal call may nevertheless place a target in the general vicinity of a shooting, narcotics delivery, or other criminal event.]**

4. Disclosure of this application, the court's order, or the fact that the requested records have been produced to the **[LAW ENFORCEMENT AGENCY]** may seriously jeopardize this pending criminal investigation.

WHEREFORE, applicant requests the Court to enter the attached Order requiring **[PROVIDER]** to disclose to **[LAW ENFORCEMENT AGENCY]** records reflecting the location of cellular towers (cell site and sector/face) related to the use of a cellular telephone assigned the telephone number **(XXX) XXX-XXXX** for the period from **[DATE 1]** to **[PRESENT/DATE 2]**; (2) precluding the provider of such service from disclosing to the

subscriber or customers or to any other unauthorized person this request, any court order issued in connection with this request, the fact of disclosure of such records to [LAW ENFORCEMENT AGENCY] or the existence of this investigation, pursuant to 18 U.S.C. § 2705(b); and (3) sealing the government's application, the Court's Order (except for the original Service Provider Order to be served on [PROVIDER]), and any related documents until otherwise ordered by the Court.

Executed on [DATE].

[NAME]
United States Attorney

By:

[NAME]
Assistant United States Attorney

IN THE UNITED STATES DISTRICT COURT FOR THE
____ DISTRICT OF ____

IN THE MATTER OF THE APPLICATION)	
OF THE UNITED STATES OF AMERICA)	
FOR AN ORDER PURSUANT TO 18 U.S.C.)	No:
§ 2703(d) DIRECTING [PROVIDER])	
TO PROVIDE HISTORICAL CELL)	
SITE LOCATION RECORDS RELATED)	<u>UNDER SEAL</u>
TO TELEPHONE NUMBER)	
[(XXX) XXX-XXXX])	

ORDER

This matter having come before the Court pursuant to an application under Title 18, United States Code, Section 2703(c)-(d) for an order directing [PROVIDER]; an electronic communication service within the meaning of 18 U.S.C. § 2510(15), to disclose to [LAW ENFORCEMENT AGENCY] records reflecting the location of cellular towers (cell site and sector/face) related to the use of a cellular telephone assigned the telephone number (XXX) XXX-XXXX for the period from [DATE 1] to [PRESENT/DATE 2], the Court finds that the applicant has offered specific and articulable facts showing that there are reasonable grounds to believe that the records and other information sought are relevant and material to an ongoing criminal investigation.

The Court further finds that prior notice of this Order (or the underlying application and investigation) to any person would seriously jeopardize the investigation.

Accordingly, IT IS ORDERED pursuant to Title 18, United States Code, Section 2703(c)-(d) that [PROVIDER] will, within ____ days of the date of this Order, disclose to [LAW ENFORCEMENT AGENCY] records reflecting the location of cellular towers (cell site and sector/face) related to the use of a cellular telephone assigned the telephone number (XXX)

XXX-XXXX for the period from **[DATE 1]** to **[PRESENT/DATE 2]**.

IT IS FURTHER ORDERED that the application and this Order (except for the original Service Provider Order to be served on **[PROVIDER]**) are sealed until otherwise ordered by this Court, and that **[PROVIDER]** shall not disclose the existence of the investigation, the application, or this Order to the listed subscriber or to any other person, unless and until authorized to do so by the Court.

SO ORDERED:

[NAME]
United States Magistrate Judge

Date: _____, 200_

“Tower Dump” Application and Order

This form is intended for use in the special circumstance where historical cell tower records are sought not for a specific phone, but rather for a specific time and location where a suspect phone is believed to have been used, such as at a bank robbery.

Because these types of requests, sometimes referred to colloquially as “tower dumps,” may produce substantial amounts of information, such requests should seek records for a relatively narrow time frame. If the target’s known calls can be characterized in objectively measurable terms – for example, calls of more than a certain length, or multiple outbound calls within a specified time frame – it is good practice to ask the provider to make selective disclosures after filtering out records not meeting those criteria.

Applicants with additional questions are encouraged to contact the author of this form (Mark Eckenwiler, Associate Director, Office of Enforcement Operations, (b) (6), (b) (7)(C) or mark.eckenwiler@usdoj.gov).

Revised 8-21-09

current version at <http://dojnet.doj.gov/usao/eousa/ole/usabook/cell/01cell05.wpd>

IN THE UNITED STATES DISTRICT COURT
FOR THE _____ DISTRICT OF _____

IN THE MATTER OF THE APPLICATION)	
OF THE UNITED STATES OF AMERICA)	Case No. _____
FOR AN ORDER PURSUANT TO)	
18 U.S.C. §§ 2703(c) & 2703(d) DIRECTING)	<u>FILED UNDER SEAL</u>
AT&T, SPRINT NEXTEL, T-MOBILE, AND)	
VERIZON WIRELESS TO DISCLOSE CELL)	
TOWER LOG INFORMATION)	
_____)	

APPLICATION

The United States of America, through _____, United States Attorney for the _____ District of _____, and his assistant, _____, Assistant United States Attorney, hereby moves this Court pursuant to 18 U.S.C. §§ 2703(c) and 2703(d) for an Order:

(1) requiring AT&T, SPRINT NEXTEL, T-MOBILE, and VERIZON WIRELESS, providers of electronic communication service within the meaning of 18 U.S.C. § 2510(15), to disclose provide historical cell tower log information as follows: records identifying any wireless telephone call (including the number of the locally-served wireless telephone and the number calling or called by it) utilizing the cellular tower servicing calls to and from [ADDRESS, CITY, STATE] at any point during the time period from [TIME 1] to [TIME 3] on [MONTH/DAY/YEAR], including but not limited to calls initiated before or terminated after the specified time period (hereinafter "the Requested Cell Tower Log Information");

(2) precluding the named providers from disclosing to the subscriber or customers or to any other person this Application, any order issued in connection with this Application, or the fact of

disclosure of such records to the requesting governmental entities or the existence of this investigation, pursuant to 18 U.S.C. § 2705(b); and

(3) sealing this Application, the Court's Order, and any related documents.

In support of this application, the undersigned states as follows:

1. The undersigned is an attorney for the government as defined by Rule 1(b)(1) of the Federal Rules of Criminal Procedure and therefore pursuant to 18 U.S.C. § 2703(c)-(d) may apply for an Order as requested herein.

2. The undersigned states that [AGENCY] is conducting an investigation involving unknown individuals in connection with criminal offenses including, among others, 18 U.S.C. § 2113 (Bank Robbery); that it is believed that a subject or subjects of the investigation used a cellular telephone in the vicinity of [ADDRESS, CITY, STATE] at the time of the target offenses; and that the information likely to be obtained from Requested Cell Tower Log Information is relevant and material to the ongoing criminal investigation.

3. In support of its request for an Order directing the disclosure of the Requested Cell Tower Log 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:

- a. On [MONTH/DAY/YEAR], at approximately [TIME 2], two unknown individuals robbed the ____ Bank at [ADDRESS, CITY, STATE], escaping with \$ _____. Witness statements and video surveillance document that one of the perpetrators was using a cell phone to make or receive a call during the robbery.
- b. [additional facts as appropriate]

4. Cell tower log information for the time period shortly before and after [TIME 2] – that is, the period from [TIME 1] to [TIME 3] on [MONTH/DAY/YEAR] – may reveal the cellular telephone number used by the perpetrator during the robbery, and therefore aid in identifying one or more of the perpetrators.

5. Disclosure of this Application, the Court's Order, or the fact that Requested Cell Tower Log Information has been disclosed to the Government may seriously jeopardize this pending criminal investigation.

WHEREFORE, applicant requests the Court to enter the attached Order, (1) requiring AT&T, T-Mobile, Sprint Nextel, and Verizon Wireless, providers of electronic communication service within the meaning of 18 U.S.C. § 2510(15), to disclose to [AGENCY] the Requested Cell Tower Log Information; (2) precluding the named providers from disclosing to the subscriber or customers or to any other person this Application, any order issued in connection with this Application, or the fact of disclosure of such records to the requesting governmental entities or the existence of this investigation, pursuant to 18 U.S.C. § 2705(b); and (3) sealing this Application, the Court's Order, and any related documents.

The foregoing is true and correct to the best of Applicant's knowledge.

[NAME]
Assistant United States Attorney

[DATE]

IN THE UNITED STATES DISTRICT COURT
FOR THE _____ DISTRICT OF _____

IN THE MATTER OF THE APPLICATION)	
OF THE UNITED STATES OF AMERICA)	Case No. _____
FOR AN ORDER PURSUANT TO)	
18 U.S.C. §§ 2703(c) & 2703(d) DIRECTING)	<u>FILED UNDER SEAL</u>
AT&T, SPRINT NEXTEL, T-MOBILE AND)	
VERIZON WIRELESS TO DISCLOSE)	
CELL TOWER LOG INFORMATION)	
_____)	

ORDER

This matter having come before the court pursuant to an Application under 18 U.S.C. §§ 2703(c)(1)(B) and 2703(d) by Assistant United States Attorney _____, an attorney for the Government as defined by Fed. R. Crim. P. 1(b)(1), requesting an Order

(1) requiring AT&T, SPRINT NEXTEL, T-MOBILE, and VERIZON WIRELESS, providers of electronic communication service within the meaning of 18 U.S.C. § 2510(15), to disclose provide historical cell tower log information as follows: records identifying any wireless telephone call (including the number of the locally-served wireless telephone and the number calling or called by it) utilizing the cellular tower servicing calls to and from [ADDRESS, CITY, STATE] at any point during the time period from [TIME 1] to [TIME 3] on [MONTH/DAY/YEAR], including but not limited to calls initiated before or terminated after the specified time period (hereinafter “the Requested Cell Tower Log Information”);

(2) precluding the named providers from disclosing to the subscriber or customers or to

any other person this Application, any order issued in connection with this Application, or the fact of disclosure of such records to the requesting governmental entities or the existence of this investigation, pursuant to 18 U.S.C. § 2705(b); and

(3) sealing this Application, the Court's Order, and any related documents,

UPON REVIEW OF THE APPLICATION, THE COURT HEREBY FINDS THAT pursuant to 18 U.S.C. §§ 2703(c)(1)(B) and 2703(d), Applicant has set forth specific and articulable facts showing that there are reasonable grounds to believe that the Requested Cell Tower Log Information is relevant and material to an ongoing criminal investigation of criminal offenses including, among others, 18 U.S.C. § 2113 (Bank Robbery).

Accordingly, IT IS ORDERED, pursuant to 18 U.S.C. §§ 2703(c)(1)(B) and 2703(d), that AT&T, Sprint Nextel, T-Mobile, and Verizon Wireless shall disclose to [AGENCY] the Requested Cell Tower Log Information.

Good cause having been shown, IT IS FURTHER ORDERED, pursuant to 18 U.S.C. § 2705(b), that this Order and the underlying Application be sealed until further order of the Court and that the named carriers and their representatives, agents and employees shall not disclose in any manner, directly or indirectly, by any action or inaction, the existence of this Order or the existence of the above-described investigation to any person unless or until otherwise ordered by the court.

DATE: _____

UNITED STATES MAGISTRATE JUDGE

Prospective Iridium Satellite Phone Location Information

The attached forms are intended for use in requesting future location information – precise only to within a few kilometers at best – concerning an Iridium satellite phone.

Questions or requests for advice may be directed to OEO Associate Director Mark Eckenwiler at (b) (6), (b) (7)(C) or mark.eckenwiler@usdoj.gov.

Revised 8-19-09

Current version available at <http://dojnet.doj.gov/usao/eousa/ole/usabook/cell/01cell06.wpd>

IN THE UNITED STATES DISTRICT COURT

FOR THE ___ DISTRICT OF ___

IN THE MATTER OF THE APPLICATION)
OF THE UNITED STATES OF AMERICA)
FOR AN ORDER AUTHORIZING THE)
INSTALLATION AND USE OF A PEN)
REGISTER AND TRAP AND TRACE)
DEVICE AND ACQUISITION OF)
LOCATION INFORMATION FOR IRIDIUM)
SATELLITE TELEPHONE)
[WITH IMSI NUMBER])

UNDER SEAL

NO. _____

APPLICATION

_____, an attorney of the United States Department of Justice, hereby applies to the Court pursuant to 18 U.S.C. §§ 3122, 3123, and 2703(d) for an Order 1) authorizing the installation and use of a pen register and trap and trace device ("Pen/Trap") on the Iridium satellite telephone bearing number _____ and IMSI _____ (the "Target Telephone") and 2) authorizing acquisition of information reflecting the approximate location of the Target Telephone (not to include GPS or other precise location information). In support of this application, Applicant states the following:

1. Applicant is an "attorney for the Government" as defined in Fed. R. Crim. P. 1, and therefore may apply, pursuant to 18 U.S.C. §§ 2703(d) and 3122, for an Order authorizing the installation and use of a Pen/Trap and acquisition of the requested location information.

2. Pursuant to 18 U.S.C. § 3123(a)(1), upon an application made under 18 U.S.C. § 3122(a)(1) a court "shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device anywhere within the United States, if the court finds that the attorney

for the Government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.”

3. Pursuant to 18 U.S.C. § 2703(d), a court may order an electronic communication service to disclose non-content information about a customer or subscriber if the government “offers specific and articulable facts showing that there are reasonable grounds to believe that the . . . records or other information sought are . . . relevant and material to an ongoing criminal investigation.”

4. Iridium Satellite LLC (“Iridium”), a satellite phone service provider based in Tempe, Arizona, routinely creates and maintains in the regular course of its business various records concerning its customers’ usage. These records typically include for each communication a customer makes or receives (1) the date and time of the communication ; (2) the telephone numbers involved; (3) the duration of the communication; and (4) the approximate terrestrial location of the telephone (to within a few kilometers).

5. By this application, the government seeks an order authorizing (1) the installation and use of a Pen/Trap on the Target Telephone and (2) the acquisition of approximate location information related to the use of the Target Telephone. The requested information does not include GPS or other precise location information.

6. Applicant certifies that the [AGENCY NAME] (the “Investigative Agency”) is conducting an ongoing criminal investigation of [TARGET NAMES], and others both known and as yet unknown, in connection with possible violations of ___ U.S.C. § _____. It is believed that one or more subjects of the investigation possess and are using the Target Telephone, which is subscribed to by [SUBSCRIBER NAME] , [SUBSCRIBER ADDRESS], with service provided by Iridium.

7. Further, as required under 18 U.S.C. § 2703(d), Applicant offers the following specific and articulable facts showing that there are reasonable grounds to believe that the requested location information is relevant and material to this ongoing criminal investigation.

8. **[Set out specific facts explaining the relevance of the requested location information. It is not necessary to show that the communications themselves are expected to be in furtherance of the offenses under investigation; for example, location records for a non-criminal call may nevertheless place a target in the general vicinity of a narcotics delivery or other criminal event.]**

#. Because Iridium's assistance will be necessary to accomplish the objectives of the requested order, Applicant further requests that the Order direct that, upon service of the order upon it, Iridium furnish information, facilities, and technical assistance necessary to accomplish the installation of the Pen/Trap, including installation and operation of the devices unobtrusively and with a minimum of disruption of normal service. Iridium shall be compensated by Investigative Agency for reasonable expenses incurred in providing such facilities and assistance in furtherance of the Order.

#. Notification to the subscriber or customer or to any other unauthorized person of the issuance of the anticipated Order (or the existence of the investigation) would seriously jeopardize said investigation. Due to the sensitive nature of this investigation and in order to protect the sources and methods involved in this investigation, it is respectfully requested that, pursuant to 18 U.S.C. § 3123(d), the Application and anticipated Order in this matter be filed under seal, until further order of this Court. For the same reasons, it is also respectfully requested that pursuant to 18 U.S.C. §§ 2705(b) and 3123(d), this Court order Iridium not to disclose the existence of the application, the

resulting court order, or the investigation to the listed subscriber for any reason or to any other person, except as required to execute the order, unless or until ordered by this Court.

WHEREFORE, IT IS REQUESTED that this Court enter an ex parte Order for a period of sixty (60) days, commencing upon the date of installation of the Pen/Trap, authorizing the installation and use of a Pen/Trap to collect the dialing, routing, addressing, and signaling information (including date and time) associated with communications to or from the Target Telephone.

IT IS FURTHER REQUESTED that the Order authorize agents of the Investigative Agency to acquire, during the same 60-day period, information reflecting the approximate location of the Target Telephone (not to include GPS or other precise location information).

IT IS FURTHER REQUESTED that the Order direct Iridium to furnish agents of the Investigative Agency forthwith all information, facilities, and technical assistance necessary to effectuate the Order unobtrusively and with minimum interference to the services accorded to the user of the Target Telephone.

IT IS FURTHER REQUESTED that this Application and the anticipated Order of this Court be filed under seal, and that the Court direct Iridium not to disclose to any person the existence of this Application, the resulting Order, or the investigation for any reason, except as required to execute the Order, unless or until ordered otherwise by this Court.

IT IS FURTHER REQUESTED that the Court's Order apply to any changed telephone number subsequently assigned to the Target Telephone within the period of the Order.

Applicant declares and certifies, under penalty of perjury, that to the best of Applicant's knowledge and belief, the foregoing is true and correct.

[NAME]
Assistant U.S. Attorney

SUBSCRIBED and SWORN to before me this _____ day of _____, 200_.

[NAME]
UNITED STATES MAGISTRATE JUDGE

IN THE UNITED STATES DISTRICT COURT

FOR THE ___ DISTRICT OF ___

IN THE MATTER OF THE APPLICATION)
OF THE UNITED STATES OF AMERICA)
FOR AN ORDER AUTHORIZING THE)
INSTALLATION AND USE OF A PEN)
REGISTER AND TRAP AND TRACE)
DEVICE AND ACQUISITION OF)
LOCATION INFORMATION FOR IRIDIUM)
SATELLITE TELEPHONE)
[WITH IMSI NUMBER])

UNDER SEAL

NO. _____

ORDER

This matter having come before the Court pursuant to an Application under 18 U.S.C. §§ 3122, 3123, and 2703(d) by _____, Assistant United States Attorney for the ___ District of ___, which Application requests an Order authorizing the installation and use of a pen register and trap and trace device ("Pen/Trap") on the satellite telephone bearing phone number _____ and ESN/IMSI _____ (the "Target Telephone"), and the acquisition of the information reflecting the approximate location of the Target Telephone (not to include GPS or other precise location information), the Court finds:

1. The Applicant has certified that the [AGENCY NAME] (the "Investigative Agency") is conducting an ongoing criminal investigation of [TARGET NAMES], and others both known and as yet unknown, in connection with possible violations of ___ U.S.C. § ___, [OFFENSE];

2. The Applicant has further certified that one or more subjects of the investigation are believed to be using the Target Telephone, subscribed to by [SUBSCRIBER NAME], [SUBSCRIBER ADDRESS], with service provided by Iridium Satellite LLC ("Iridium"), a satellite phone service provider based in Tempe, Arizona; and

3. The Applicant has offered specific and articulable facts showing that there are reasonable grounds to believe that the requested location information is relevant and material to the ongoing criminal investigation.

IT IS THEREFORE ORDERED, pursuant to 18 U.S.C. § 3123, that agents of the Investigative Agency may, for a period of sixty (60) days commencing upon the date of installation of the Pen/Trap, install and use a Pen/Trap to collect the dialing, routing, addressing, and signaling information (including date and time) associated with communications to or from the Target Telephone.

IT IS FURTHER ORDERED that agents of the Investigative Agency are authorized to acquire, during the same 60-day period, information reflecting the approximate location of the Target Telephone (not to include GPS or other precise location information).

IT IS FURTHER ORDERED that Iridium furnish agents of the Investigative Agency forthwith all information, facilities, and technical assistance necessary to effectuate the Order unobtrusively and with minimum interference to the services accorded to the user(s) of the Target Telephone, and that Iridium be compensated by the Investigative Agency for reasonable expenses incurred in providing such facilities and technical assistance.

IT IS FURTHER ORDERED that this Order and the underlying Application be sealed, and that Iridium not disclose to any person the existence of this Order, the underlying Application, or the investigation for any reason, except as required to execute the Order, unless or until ordered otherwise by this Court.

IT IS FURTHER ORDERED that this Order apply to any changed telephone number, subsequently assigned to the Target Telephone within the period of this Order.

SIGNED this _____ day of _____, 200_.

[NAME]
UNITED STATES MAGISTRATE JUDGE

Vehicle Tracking Device Form

The forms on the following pages are designed for use in seeking authorization to install and monitor a physical tracking device in or on a vehicle. They should not be used for OnStar or with respect to a target's own cellphone (as neither is a section 3117 "tracking device" in the Department's view); separate forms for those scenarios are available elsewhere in this Appendix.

Questions or requests for advice may be directed to OEO Associate Director Mark Eckenwiler at (b) (6), (b) (7)(C) or mark.eckenwiler@usdoj.gov.

Revised 1-26-2012

Current version available at <http://dojnet.doj.gov/usao/eousa/ole/usabook/cell/02cell01.wpd>

UNITED STATES DISTRICT COURT
DISTRICT OF _____

IN THE MATTER OF THE APPLICATION)
OF THE UNITED STATES OF AMERICA)
FOR A WARRANT AUTHORIZING THE)
INSTALLATION AND MONITORING OF)
A TRACKING DEVICE IN OR ON A _____,)
LICENSE PLATE NUMBER _____,)
VIN # _____)
_____)

AFFIDAVIT

(Fed. R. Crim. P. 41;
18 U.S.C. § 3117)

(UNDER SEAL)

STATE OF _____)
COUNTY OF _____ : ss.:
_____ DISTRICT OF _____)

_____, a Special Agent with the _____, being duly sworn, deposes and states:

Upon information and belief, a _____,

bearing license plate number _____, vehicle identification number _____ ("the
subject vehicle"), is presently being used in furtherance of **[specify the crimes]**.

Your deponent further states that there is probable cause to believe that the installation of
a tracking device in or on the subject vehicle, and use of the tracking device, will lead to
evidence, fruits, and instrumentalities of the aforementioned crimes as well as to the
identification of individuals who are engaged in the commission of those and related crimes.

The source of your deponent's information and the grounds for his belief are as follows:

1. I have been a Special Agent with the _____
for _____ years, and am the case agent on this case. As the case agent, I am fully familiar with
the facts of the case:

2. On or about _____, I learned from a reliable confidential
informant ("CI") that _____ was involved in **[list the offense(s)]** in **[location]**. The CI
subsequently informed me that _____.

3. On _____, at approximately _____, I established a surveillance in the vicinity
of _____. I observed _____ leave a building located at
_____ and enter the subject vehicle.

4. A review of Department of Motor Vehicles records reveals that the subject vehicle is
registered to _____.

5. The CI has stated that _____ is using the subject vehicle in connection
with **[describe the criminal activity]**. Based upon my own observations, I know that the subject
vehicle is presently within the _____ District of _____.

6. In order to track the movement of the subject vehicle effectively and to decrease the
chance of detection, I seek to place a tracking device in or on the subject vehicle while it is in the
_____ District of _____. Because _____ sometimes parks the subject
vehicle in his driveway and on other private property, it may be necessary to enter onto private
property and/or move the subject vehicle in order to effect the installation, repair, replacement,
and removal of the tracking device. [To ensure the safety of the executing officer(s) and to avoid
premature disclosure of the investigation, it is requested that the court authorize installation and
removal of the tracking device during both daytime and nighttime hours.] **[NOTE: Include**

relevant facts such as daytime visibility of vehicle's anticipated location and/or target's possession of weapons or history of violence.]

7. In the event that the Court grants this application, there will be periodic monitoring of the tracking device during both daytime and nighttime hours for a period of **[FRCP 41(e)(2)(B) limits period to 45 days from date of issue]** days following installation of the device. The tracking device may produce signals from inside private garages or other such locations not open to the public or visual surveillance.

8. It is requested that the warrant and accompanying affidavit and application in support thereof, as they reveal an ongoing investigation, be sealed until further order of the Court in order to avoid premature disclosure of the investigation, guard against the flight of fugitives, and better ensure the safety of agents and others, except that copies of the warrant in full or redacted form may be maintained by the United States Attorney's Office, and may be served on Special Agents and other investigative and law enforcement officers of the ____, federally deputized state and local law enforcement officers, and other government and contract personnel acting under the supervision of such investigative or law enforcement officers, as necessary to effectuate the warrant.

9. In accordance with 18 U.S.C. 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), I request that the warrant delay notification of the execution of the warrant for a period not to exceed 30 days **[or a later date certain if the facts justify it]** after the end of the authorized period of tracking (including any extensions thereof) because there is reasonable cause to believe that providing immediate notification would seriously jeopardize the investigation.

WHEREFORE, your deponent respectively requests that the Court issue a warrant authorizing members of _____ or their authorized representatives, including but not limited to other law enforcement agents and technicians assisting in the above-described investigation, to install a tracking device in or on the subject vehicle within the _____ District of _____ within 10 calendar days of the issuance of the requested warrant, and to remove said tracking device from the subject vehicle after the use of the tracking device has ended; to [surreptitiously enter {specify location/address with particularity} and/or] move the subject vehicle to effect the installation, repair, replacement, and removal of the tracking device; and to monitor the tracking device, for a period of ___ days following the issuance of the warrant [FRCP 41(e)(2)(B) limits the period to 45 days from date of issue], including when the tracking device is inside private garages and other locations not open to the public or visual surveillance, both within and outside the _____ District of _____.

Special Agent

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

United States Magistrate Judge

UNITED STATES DISTRICT COURT
DISTRICT OF _____

IN THE MATTER OF THE APPLICATION)
OF THE UNITED STATES OF AMERICA)
FOR A WARRANT AUTHORIZING THE)
INSTALLATION AND MONITORING OF A)
TRACKING DEVICE IN OR ON A _____,)
LICENSE PLATE NUMBER _____,)
VEHICLE IDENTIFICATION NUMBER)
_____)
_____)

WARRANT FOR A
TRACKING DEVICE

(Fed. R. Crim. P. 41;
18 U.S.C. § 3117)

(UNDER SEAL)

WHEREAS an affidavit has been presented to the Court by Special Agent
_____ of the _____, and full consideration having been given to
the matters set forth therein, this Court finds that there is probable cause to install and use a
tracking device in or on a vehicle described as a _____, license plate
number _____, vehicle identification number _____ ("the subject vehicle"), and
that the use of such tracking device will lead to evidence, fruits, and instrumentalities of
_____ [specify offenses].

IT IS HEREBY ORDERED, pursuant to Federal Rule of Criminal Procedure 41 and 18
U.S.C. § 3117, that Special Agent _____ of the _____, together with other
Special Agents and their authorized representatives are authorized, within ten calendar days from
the date of this warrant, to install a tracking device in or on the subject vehicle within the
_____ District of _____ [issuing district] during the daytime [unless for good
cause the judge expressly authorizes installation at another time].

It is further ORDERED that said Special Agents and their authorized representatives are
further authorized to [surreptitiously enter {specify location/address with particularity} and]

move said vehicle to effect the installation, maintenance, and removal of the tracking device.

It is further ORDERED that said Special Agents and their authorized representatives are authorized, for a period of ____ days from the date the warrant is issued [**FRCP 41(e)(2)(B) permits a reasonable length of time but no more than 45 days from the date the warrant is issued**], to monitor the tracking device installed in or on the subject vehicle, including when the subject vehicle is inside any private garage or other location not open to the public or visual surveillance, both within and outside the _____ District of _____ [**issuing district**].

It is further ORDERED that the executing officer return this warrant to the undersigned Magistrate Judge within 10 calendar days after the use of the tracking device has ended.

It is further ORDERED that this warrant and the accompanying affidavit/application submitted in support thereof, as they reveal an ongoing investigation, be sealed until further Order of the Court in order to avoid premature disclosure of the investigation, guard against the flight of fugitives, and better ensure the safety of agents and others, except that copies of the warrant in full or redacted form may be maintained by the United States Attorney's Office, and may be served on Special Agents and other investigative and law enforcement officers of the _____, federally deputized state and local law enforcement officers, and other government and contract personnel acting under the supervision of such investigative or law enforcement officers, as necessary to effectuate the warrant; and

It is further ORDERED, in accordance with 18 U.S.C. 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), that notification of the execution of this order be delayed for a period of 30 days [**or a later date certain if the facts justify it**] after the end of the authorized period of tracking (including any extensions thereof) because there is reasonable cause to believe

that providing immediate notification would seriously jeopardize the investigation.

Dated: _____, _____

UNITED STATES MAGISTRATE JUDGE

[To be entered by the executing officer]

The tracking device was installed on the following date and time:

The tracking device was used during the period starting on _____ and ending on _____.

I declare under penalty of perjury that this return is correct and was returned along with the original warrant to the designated judge.

(Executing officer)

Model Form for IP Trap and Trace on a Web-based Account

The sample application and order below are specifically designed for use to locate and/or identify the person using a specified account on a web-based service such as Yahoo, Hotmail, or Facebook. The order authorizes the collection of the numeric network address(es) — i.e., the Internet Protocol (IP) address(es) — from which the user accesses the account. That information, in turn, can be used to trace the user to the other Internet site (such as an ISP, a cybercafe, or a public library terminal) from which he or she accessed the account. It is primarily useful in cases (such as fugitive investigations) where the objective is to identify and locate the user.

Note that this order is not designed to collect the email addresses to which the user sends email messages from the web-based account, nor to collect the addresses from which the account owner receives messages. That type of order — which might be used, for example, to discover the co-conspirators of a criminal known to use email in his/her conspiratorial activities — would not ask for IP addresses, and would normally require discussion of the pen register provisions of the statute as well as trap and trace.

Revised 8-19-09

Current version available at <http://dojnet.doj.gov/usao/eousa/ole/usabook/cell/04cell01.wpd>

UNITED STATES DISTRICT COURT
DISTRICT OF _____

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

No.

FILED UNDER SEAL

APPLICATION

_____, the United States Attorney for the _____ District of _____, by
_____, an Assistant United States Attorney for the _____ District of _____,
hereby applies to the Court pursuant to 18 U.S.C. § 3122 for an order authorizing the installation
and use of a trap and trace device. In support of this application, he/she states the following:

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

2. Applicant certifies that the information likely to be obtained is relevant to an
ongoing criminal investigation being conducted by [investigative agency], in connection with
possible violations of Title 18, United States Code, sections _____.

3. [As a result of information obtained through previous orders issued by this Court,]
investigators believe that the offense under investigation has been and continues to be
accomplished through the user account _____ at _____, an electronic communication service
provider located at _____. The listed subscriber for this account is [name], [address],
[telephone]. _____, and others yet unknown, are the subjects of the above investigation.

4. A trap and trace device is defined in Title 18, United States Code, Section 3127(4)
as "a device or process which captures the incoming electronic or other impulses which identify
the originating number or other dialing, routing, addressing, and signaling information
reasonably likely to identify the source of a wire or electronic communication."

5. [provider] is a provider of [free] electronic communication services. [provider's] users access its services by means of the Internet's World Wide Web. Using a standard web browser (such as Firefox or Internet Explorer), [provider's] users may compose, send, and receive electronic messages through the computers in [provider's] network.

6. Whenever an Internet user visits [provider's] web site (or any other web site on the Internet), that user's computer identifies itself to the web site by means of its Internet Protocol address. An Internet Protocol ("IP") address is a unique numeric identifier assigned to every computer attached to the Internet. An Internet service provider (ISP) normally controls a range of several hundred (or even thousands of) IP addresses, which it assigns to its customers for their use.

7. IP numbers for individual user accounts (such as are offered by ISPs to the general public) are usually assigned "dynamically": that is, randomly from the pool of available IP addresses controlled by the ISP, and for a limited time period. (In the case of dialup users, the assignment lasts only for the duration of the call. For users connecting via broadband – e.g., DSL or cable – the assignment may last anywhere from a few hours to a month or longer, depending on the ISP's business practices.) The customer's computer retains that IP address for the duration of the assignment, and the IP address cannot be assigned to another user during that period. At the end of the limited time period (e.g., when a dialup user disconnects), that IP address reverts to the pool of unused addresses available to other customers, and the user's computer will need to request assignment of a new IP address. In short, an individual customer's IP address normally varies over time. By contrast, an ISP's business customer will commonly have a permanent, 24-hour Internet connection to which a "static" (i.e., fixed) IP address is assigned.

8. These source IP addresses are, in the computer network context, conceptually identical to the origination phone numbers captured by traditional trap and trace devices installed on telephone lines. Just as traditional telephonic trap and trace devices may be used to determine the source of a telephone call (and thus the identity of the caller), it is feasible to use a combination of hardware and software to ascertain the source addresses of electronic connections

to a World Wide Web computer, and thereby to identify and locate the originator of the connection.

9. Accordingly, for the above reasons, the applicant requests that the Court enter an order authorizing the installation and use of a trap and trace device to identify the source IP address (along with the date and time) of all logins to the subscriber account [user account] at [provider]. The applicant is not requesting, and does not seek to obtain, the contents of any communications.

10. The applicant requests that the foregoing installation and use be authorized for a period of 60 days.

11. The applicant further requests that the Order direct that, upon service of the order, [provider] furnish information, facilities, and technical assistance necessary to accomplish the installation of the trap and trace device, including installation and operation of the device unobtrusively and with a minimum of disruption of normal service. [provider] shall be compensated by [investigating agency] for reasonable expenses incurred in providing such facilities and assistance in furtherance of the Order.

12. The applicant further requests that the Order direct that the information collected and recorded pursuant to the Order be furnished to [investigating agency] at reasonable intervals during regular business hours for the duration of the Order.

13. The applicant further requests that the Order direct that the tracing operation encompass tracing the communications to their true source, if possible, without geographic limit.

14. The applicant further requests that pursuant to Title 18, United States Code, Section 3123(d)(2) the Court's Order direct [provider]; and any other person or entity providing wire or electronic communication service in the United States whose assistance is used to facilitate the execution of this Order, and their agents and employees not to disclose to the listed subscriber, or any other person, the existence of this Order, the trap and trace device, or this investigation unless or until otherwise ordered by the court and further, pursuant to Title 18, United States Code, Section 3123(d)(1), that this application and Order be SEALED.

The foregoing is based on information provided to me in my official capacity by agents of [investigative agency].

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

Dated this _____ day of _____, 200_.

Assistant United States Attorney

UNITED STATES DISTRICT COURT
DISTRICT OF _____

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

No.

FILED UNDER SEAL

ORDER

This matter has come before the Court pursuant to an application under Title 18, United States Code, Section 3122 by _____, 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 trap and trace device to determine the source Internet Protocol address (along with date and time) of login connections directed to the user account _____ at [provider name], which is located at [address of provider]. The account is registered to [name/address].

The Court finds that the applicant has certified that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation into possible violations of Title 18, United States Code, Section _____, by _____ [and others yet unknown].

IT IS THEREFORE ORDERED, pursuant to Title 18, United States Code, Section 3123, that a trap and trace device be installed and used to determine the source Internet Protocol address (along with date and time) of login connections directed to the user account [user account], but not the contents of such communications;

IT IS FURTHER ORDERED, pursuant to Title 18, United States Code, Section 3123(c)(1), that the use and installation of the foregoing occur for a period not to exceed 60 days;

IT IS FURTHER ORDERED, pursuant to Title 18, United States Code, Section

3123(b)(2) and in accordance with the provisions of section 3124(b), that [provider], upon service of the order upon it, shall furnish information, facilities, and technical assistance necessary to accomplish the installation of the trap and trace device, including installation and operation of the device unobtrusively and with a minimum of disruption of normal service;

IT IS FURTHER ORDERED, that the results of the trap and trace device shall be furnished to [agency] at reasonable intervals during regular business hours for the duration of the Order;

IT IS FURTHER ORDERED, that the tracing operation shall encompass tracing the communications to their true source, if possible, without geographic limit;

IT IS FURTHER ORDERED that [agency] compensate [provider] for expenses reasonably incurred in complying with this Order; and

IT IS FURTHER ORDERED, pursuant to Title 18, United States Code, Section 3123(d), that [insert provider name], and any other person or entity providing wire or electronic communication service in the United States whose assistance is used to facilitate the execution of this Order, and their agents and employees shall not disclose to the listed subscriber, or any other person, the existence of this Order, the trap and trace device, or this investigation unless or until otherwise ordered by the court and further, pursuant to Title 18, United States Code, Section 3123(d)(1), that this application and Order be SEALED

Dated this _____ day of _____, 200_.

UNITED STATES MAGISTRATE JUDGE

[USABook](#) > [Drugs](#) > [Federal Narcotics Manual](#) > **Chapter 3**
[prev](#) | [next](#) | [help](#) | [download](#)

Chapter 3

Electronic Surveillance— Non-Wiretap

Joshua P. Jones
Trial Attorney
Narcotic and Dangerous Drug Section

3.1	Resources
3.2	Overview
3.3	Pen registers and trap and trace devices—generally
3.4	Pen registers and trap and trace devices—application and order
3.5	Pen registers and trap and trace devices—email and Internet
3.6	Pen registers and trap and trace devices—emergency surveillance
3.7	Electronic tracking devices—generally
3.8	Cellular telephone location information
3.9	Consensual monitoring
3.10	Video surveillance
3.11	Other electronically-enhanced surveillance techniques

3.1

Resources

- Electronic Surveillance Unit (ESU), [Office of Enforcement Operations \(OEO\)](#), Criminal Division, at (202) 514-6809.
- The OEO publishes three manuals that are regularly updated and posted on USABook: the *Electronic Surveillance Manual*, <http://dojnet.doj.gov/usao/eousa/ole/usabook/elsu>, *Electronic Surveillance Issues*, <http://dojnet.doj.gov/usao/eousa/ole/usabook/esis>, and *Tracking Devices, Cell Phones, and Other Location Technologies*, <http://dojnet.doj.gov/usao/eousa/ole/usabook/cell>.
- Fishman & McKenna, [Wiretapping and Eavesdropping: Surveillance in the Internet Age](#) (3d Edition 2008).
- *Georgetown Law Journal Annual Review of Criminal Procedure*, and particularly the chapter on "Electronic Surveillance." See the discussion of its availability in hard copy, and electronically on USABook at <http://dojnet.doj.gov/usao/eousa/ole/usabook/geor>.
- *United States Attorneys' Manual Chapter 9-7.000* ("Electronic Surveillance"), and the *Criminal Resource Manual* at 27-37 and 89-92 available at http://www.justice.gov/usao/eousa/foia_reading_room/usam.
- The Criminal Division's Office of Enforcement Operations (OEO) and Computer Crime and Intellectual Property Section (CCIPS) publish newsletters. Instructions

on how to subscribe can be found at
<http://dojnet.doj.gov/usao/eousa/ole/tables/subject/elsu.htm#manuals>.

- USABook Electronic Surveillance topic page on DOJNet at <http://dojnet.doj.gov/usao/eousa/ole/tables/subject/elsu.htm>.
- Forms that may be used to obtain judicial non-wiretap electronic surveillance authority may be found on DOJNet at <http://dojnet.doj.gov/usao/eousa/ole/usabook/elsu/20elsu.htm>, <http://dojnet.doj.gov/usao/eousa/ole/usabook/drug/forms>, and <http://dojnet.doj.gov/usao/eousa/ole/usabook/cell>.

3.2

Overview

Non-wiretap electronic surveillance measures include the use of pen registers and trap and trace devices; cell-site, GPS, or other methods of tracking or locating a criminal suspect; consensual monitoring of oral, wire, or electronic communications; or physical surveillance conducted through enhanced visual or thermal imaging devices. Such measures may be employed as precursors to a Title III wiretap application or presented as corroborating evidence of criminal activity at trial.

With the 2001 passage of the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*, Public Law 107- 56 (USA PATRIOT Act), and advances in cell site, GPS and other electronic tracking and surveillance technology, case law relevant to such methods is developing and may not be consistent from jurisdiction to jurisdiction. This Chapter summarizes prevailing case law at the time of the publication of this edition. The most up-to-date guidance may be sought from OEO at (202) 514-6809.

3.3

Pen registers and trap and trace devices—generally

westlaw query "pen register" "trap and trace"

"Pen register" authority for cellular telephones is carried out using a cellular telephone digital analyzer, which allows agents to monitor telephone usage in real time from the wire rooms at their offices. The information may be used to support probable cause for a Title III wiretap application, as corroborating evidence of guilt at trial, or to identify the associates of a criminal investigation target. With non-cellular telephone usage, a pen register, also called a dialed number recorder or, with a touch-tone telephone, a touch-tone recorder, is the device that records the numbers dialed from a land line telephone. A trap and trace device records the numbers associated with telephones calling into a particular land line telephone.

Practice note. Agents may obtain the same information available from pen registers, trap and trace devices, or digital analyzers through a toll record subpoena of the relevant service provider under 18 U.S.C. § 2703(c), with or without a court order. While the toll record subpoenas do not allow for real-time monitoring of telephone usage, the subpoenas may provide a more cost-effective and time-efficient way of obtaining toll data to be used in support of a Title III application. Stored email content older than 180 days may be obtained by § 2703 subpoena as well. Opened email less than 180 days old may be obtained via § 2703 subpoena subject to the notice requirements set forth in § 2703(b)(1)(B). *see Rehberg v. Paulk*, 611 F.3d 828 (11th Cir. 2010) ("No Supreme Court decision and no precedential decision of this Circuit defines privacy rights in e-mail content voluntarily transmitted over the global Internet and stored at a third party ISP [The plaintiff] has not identified any judicial decision holding a

government agent liable for Fourth Amendment violations related to e-mail content received by a third party and stored on a third party's server."). *But see Theofel v. Farey-Jones*, 359 F.3d 1066, 1077 (9th Cir. 2004) (holding that opened, as well as unopened, email stored on Internet service provider's server are covered under Stored Communications Act). *Theofel* has not been followed in other circuits. *See, e.g., United States v. Weaver*, 636 F.Supp.2d 769 (C.D. Ill. 2009) (distinguishing *Theofel* in cases of Web-based email such as Hotmail, and finding *Theofel* "unpersuasive" otherwise). Stored wire communications, such as voicemail, may be obtained under § 2703 or by issuance of a search warrant.

The current statutory framework providing for the authorization of pen registers and trap and trace devices, codified at 18 U.S.C. §§ 3121-27, was established under the Electronic Communications Privacy Act of 1986 and substantially modified by the USA PATRIOT Act of 2001. The statute defines a pen register as "any 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." 18 U.S.C. § 3127(3). A trap and trace device is defined as any "device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication." *Id.* § 3127(4). The 2001 amendments to the statutory definitions clarified that cellular telephone digital analyzers are covered under the statute and provided for the acquisition of non-content information from email accounts and other forms of electronic communications. The application of §§ 3121-27 to email accounts is discussed in Section 3.5 of this Chapter.

Pen register or trap and trace authority under §§ 3121-27 allows for the collection of information related to the identity of the participants in a telephone, text, or email communication, but it *never* extends to the content of any communication. *See 18 U.S.C. § 3127(3), (4)* (providing that pen register and trap and trace information "shall not include the contents of any communication"). The 2001 USA PATRIOT Act amendments provided that agents "shall use technology reasonably available" to restrict recorded information to "the dialing, routing, addressing, and signaling information used 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).

In the course of conducting pen register or trap and trace surveillance on telephones, agents sometimes encounter "post-cut-through dialed digits," which are digits 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 identifies the device to which the call is being placed. Under these circumstances, the "post-cut-through" digits may be captured by agents under the statute because they are non-content. At other times, however, "post-cut-through dialed digits" may represent call content, such as when a person dials the telephone number of the pager and subsequently enters a numerical message for the user or when a person enters personal identification, passwords, or account numbers in calls to automated banking systems. Such data would constitute "content" and should not be recorded or, if recorded inadvertently, used to further an investigation.

Subsequent to the USA PATRIOT Act amendments, Deputy Attorney General Larry Thompson set forth the Department of Justice policy regarding "over collection" of data through pen registers and trap and trace devices in a May 24, 2002 memorandum, available on DOJNet at <http://dojnet.doj.gov/usao/eousa/ole/tables/misc/penreg.pdf>. The memorandum requires affirmative steps by law enforcement agencies to avoid the collection of content information under pen register or trap and trace orders. If content is inadvertently collected, the memorandum requires that there be no affirmative investigative use of the content information.

The memorandum provides that the definition of "content" should be guided by Title III, which defines "content" as "any information concerning the substance, purport, or meaning of [a] communication." 18 U.S.C. § 2510(8). The pen register and trap and trace definitions in § 3127 indicate that "dialing, routing, addressing or signaling information" used in "processing and transmitting" wire or electronic communications does not, without more, constitute "content." 18 U.S.C. § 3127(3). If issues arise concerning whether a particular type of communication constitutes "content," prosecutors should contact OEO for wire communications or the Computer Crime and Intellectual Property Section (CCIPS) for computer-oriented communications.

Practice note. Technology is available to limit the pen register device so that it only records a specified number of dialed digits, such as the first ten digits (for domestic telephone calls, or more than ten digits for international calls). While this may eliminate the inadvertent collection of the "content" of a communication, it may also eliminate the collection of legitimate, lawful data pertinent to an investigation, such as when additional number sequences are necessary in order for a telephone user to contact a recipient.

Prosecutors should be aware of the steps that investigative agents may take to prevent over collection of content data, and should ensure that inadvertently-collected content data is not used in affidavits, court filings, or otherwise to further an investigation.

In *Smith v. Maryland*, 442 U.S. 735 (1979), the Supreme Court held that law enforcement agents need not obtain a search warrant before employing a pen register to ascertain numbers dialed from a particular telephone. The Court noted that the Fourth Amendment regulates governmental conduct only where such conduct intrudes upon a person's reasonable expectation of privacy, and that when a person voluntarily reveals information to a third person, he assumes the risk that the third person will reveal the information to the government. *Id.* at 743-44. When a person uses a telephone, he "voluntarily convey[s] numerical information to the telephone company and 'expose[s]' that information; he therefore assume[s] the risk that the company [will] reveal to the police the numbers he dialed." *Id.* at 745. Thus, the collection of non-content information via pen registers or similar devices or processes does not implicate Fourth Amendment concerns and does not require electronic surveillance authority under Title III.

Courts have accordingly held that information gathered from pen registers or trap and trace devices, even if obtained in violation of applicable statutes, is not excludable under the Fourth Amendment and may be submitted as evidence at trial. *E.g.*, *United States v. German*, 486 F.3d 849 (5th Cir. 2007); *United States v. Fregoso*, 60 F.3d 1314 (8th Cir. 1995).

3.4

Pen registers and trap and trace devices—application and order

While, under *Smith*, the use of a pen register or similar device or process for the collection of telephone toll data does not implicate constitutional concerns, 18 U.S.C. § 3121 does prohibit the installation or use of such a device or process without court authorization. Such court authorization may be sought under § 3122, which requires that an application include (1) the identity of the government attorney and law enforcement agency making the application and (2) certification by the applicant that any information obtained under the order is relevant to an ongoing criminal investigation being conducted by the agency. The statute does not require a statement of facts establishing probable cause or reasonable suspicion to believe that the information obtained will be relevant to an ongoing investigation; the statute only requires a certification to that effect.

The application is made by the government attorney under oath, and it should be made to a court "of competent jurisdiction." 18 U.S.C. § 3122(a)(1). The USA PATRIOT

Act of 2001 revised the definition of "court of competent jurisdiction," codified at 18 U.S.C. § 3127(2)(A), to include "any district court of the United States (including a magistrate judge of such a court) ... having jurisdiction over the offense being investigated." Thus, the revised definition involves "a new nexus standard under § 3127 (2)(A) [providing] that the issuing court must have jurisdiction over the crime being investigated rather than the communication line upon which the device is to be installed." H. Rep. 107-256, at 53 (2001).

Upon application under § 3122, the district court "shall enter an ex parte order authorizing the installation and use of a pen register or a trap and trace device within the jurisdiction of the court" if the court finds that a government attorney or investigative officer has certified that information obtained will be relevant to an ongoing criminal investigation. "The provision does not envision an independent judicial review of whether the application meets the relevance standard, rather the court needs only to review the completeness of the certification submitted." Senate Rep. No. 99-541 at 47.

The § 3123 order should specify:

- (A) the identity, if known, of the telephone subscriber;
- (B) the identity, if known, of the subject of the criminal investigation;
- (C) the number and, if known, physical location of the telephone; and
- (D) the criminal offense to which the information sought relates.

18 U.S.C. § 3123(b).

The order also "shall direct" that the matter be sealed and that third-party telephone companies may not reveal to anyone the existence of the order "unless or until otherwise ordered by the court." 18 U.S.C. § 3123(d)(2). The § 3123 order permits collection of data "for a period not to exceed sixty days." 18 U.S.C. § 3123(c)(1). Extensions of sixty days may be granted upon new application. *Id.* § 3123(c)(2).

Courts have observed that the "judicial role in approving use of" pen registers or trap and trace devices is "ministerial in nature." *United States v. Fregoso*, 60 F.3d 1314, 1320 (8th Cir. 1995); *United States v. Hallmark*, 911 F.2d 399, 402 (10th Cir. 1990). Thus, it is inappropriate for a court to require the showing of a factual foundation supporting its request for pen register or trap and trace authority. *United States v. Doe*, 967 F.2d 593 (9th Cir. 1992) (unpublished opinion). "[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." *Hallmark*, 911 F.2d at 402.

The terms of a third-party service provider's compliance with court orders are set forth in 18 U.S.C. § 3124. The provider is required to furnish agents with "all information, facilities, and technical assistance necessary to accomplish the installation of the pen register unobtrusively and with a minimum of interference." 18 U.S.C. § 3124(a).

3.5

Pen registers and trap and trace devices—email and Internet

The USA PATRIOT Act of 2001 amended 18 U.S.C. §§ 3121-27 to clarify the statutes' application to email, the Internet, and other forms of electronic communications. As with other forms of information obtainable under § 3123, authorization for email or Internet pen registers does not extend to content information. As noted in Section 3.3 of this Chapter, the government is required by law and Department policy to use the latest available technology in excluding content

information (e.g., 18 U.S.C. § 3121(c)). Because information disseminated by Internet service providers related to email headers or URLs accessed by an Internet user may include a "subject line" or other content information, steps should be taken by the Internet service provider to ensure that the records it provides to agents excludes such content information. See *In re Application of U.S. for an Order Authorizing use of a Pen Register and Trap*, 396 F.Supp. 45, 49-50 (D. Mass. 2005) (outlining potential problems in provision of information by Internet service provider and suggesting clarification language for orders); accord, *In the Matter of Application of the United States of America for an Order Authorizing the Installation and Use of a Pen Register and a Trap & Trace Device on Email Account*, 416 F.Supp.2d 13, 18 (D.D.C. 2006). Pen registers also should not be used to collect Uniform Resource Locators (URLs), commonly referred to as web addresses, without prior consultation with CCIPS, per USAM 9-7.500.

The Ninth Circuit has held that electronic surveillance techniques revealing "to/from addresses of email messages, the IP addresses of websites visited and the total amount of data transmitted to or from an account" are "constitutionally indistinguishable from the use of a pen register." *United States v. Forrester*, 512 F.3d 500, 510-11 (9th Cir. 2008).

Practice note. Law enforcement agencies alternatively may obtain access to content information for opened email under 18 U.S.C. § 2703(b), which sets forth the standards for 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." Under § 2703(a), disclosure of communications in "electronic storage" (e.g., unopened e-mail or "backup storage" of email) for 180 days or less may be compelled only by means of a search warrant; disclosure of communications stored with a "remote computing service" (e.g., opened e-mail) may be compelled by subpoena. *But see Theofel v. Farey-Jones*, 359 F.3d 1066, 1073 (9th Cir. 2004) ("Permission to access a stored communication does not constitute valid authorization if it would not defeat a trespass claim in analogous circumstance.")

Notice requirements may apply when a subpoena is sought to compel the production of opened email less than 180 days old. 18 U.S.C. § 2703(b)(1)(B). To delay notice disclosure requirements and obtain a statutory non-disclosure order applicable to content information furnished under 18 U.S.C. § 2703, an application for non-disclosure may be submitted to the court 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(a).

Further information and resources can be found on DOJNet at <http://dojnet.doj.gov/usao/eousa/ole/tables/subject/sca.htm>. See also the CCIPS forms at <http://dojnet.doj.gov/criminal/ccips/online/2703.htm>, and Forms 316-317 at <http://dojnet.doj.gov/usao/eousa/ole/usabook/drug/forms>.

3.6

Pen registers and trap and trace devices—emergency surveillance

westlaw query 18 +s 3125 /p emergency "special designation"

Under 18 U.S.C. § 3125, agents, upon "special designation" by the Attorney General, Deputy Attorney General, Associate Attorney General, Assistant Attorney General, or Deputy Assistant Attorney General, may obtain emergency authority to implement a pen register or trap and trace device. Such authority may be exercised in

cases of immediate danger of death or serious bodily injury to any person, conspiratorial activities "characteristic of organized crime," an immediate threat to a national security interest, or an ongoing attack against a protected computer that would constitute a felony. 18 U.S.C. § 3125(a). In such cases, court authorization must be obtained within forty-eight hours after implementing the device. If such authorization is not obtained, use of the pen register or trap and trace device should cease prior to the expiration of the forty-eight hour period. *Id.* § 3125(b). Requests for emergency pen register and trap and trace authorization should be made by an Assistant United States Attorney and directed to the Electronic Surveillance Unit at OEO (202-514-6809, or, after hours, through the Department of Justice Command Center at 202-514-5000).

3.7

Electronic tracking devices—generally

Electronic tracking, including the use of transponders or GPS devices, is commonly employed in narcotics investigations in order to locate and track shipments of illegal drugs or illegal drug proceeds. Typically, a tracking device is attached to a vehicle or other object traveling with a suspected drug trafficker. As the drug trafficker moves, the tracking device sends a signal to satellites. The location of the tracking device is then determined by obtaining longitude and latitude information from the satellites. The direction of travel and the speed the vehicle is traveling may also be inferred from the location data.

The Supreme Court has held that the use of an electronic tracking device gives rise to Fourth Amendment concerns only when the device is used to track a person within a place where the person maintains a reasonable expectation of privacy. *United States v. Knotts*, 460 U.S. 276, 281 (1983). The *Knotts* Court found that "a person traveling in an automobile on a public thoroughfare has no reasonable expectation of privacy in his movements from one place to another," and that tracking such a person's movements on public roads, whether by visual surveillance or electronic tracking, does not violate the Fourth Amendment. *Id.* Similarly, there is no Fourth Amendment violation when law enforcement agents 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).

In *United States v. Karo*, 468 U.S. 705 (1984), the Supreme Court addressed Fourth Amendment concerns in the *installation* of electronic tracking devices. The Court held that if the device is placed within a vehicle or other object without the owner's (or lawful possessor's) consent, a search warrant must be obtained describing the vehicle or object, the length of time that the device will be installed and monitored, and the factual circumstances supporting cause for the warrant. *Id.* at 718. The *Karo* Court also reiterated the rule announced in *Knotts* regarding electronic tracking in public and private locations, observing that tracking devices fall into the ambit of the Fourth Amendment when they reveal a "critical fact about the interior" of a location that could not have been discovered by unaided physical surveillance. *Karo*, 468 U.S. at 715-16.

No warrant or court order is needed to place a tracking device in a package containing contraband, stolen property or the like because an individual has no legitimate expectation of privacy in items that the individual has no right to possess at all. *United States v. Jones*, 31 F.3d 1304, 1310-11 (4th Cir. 1994); *United States v. Washington*, 586 F.2d 1147, 1154 (7th Cir. 1978); *United States v. Moore*, 562 F.2d 106, 111 (1st Cir. 1977). If the device is installed on the exterior of a vehicle while the vehicle is in a public location, no search warrant is necessary. *United States v. Garcia*, 474 F.3d 994 (7th Cir. 2007); *United States v. Michael*, 645 F.2d 252, 256 (5th Cir. 1981). Likewise, if a device is installed with the consent of a vehicle's owner and the vehicle is subsequently used by the target of a criminal investigation, the installation does not give rise to Fourth Amendment concerns. *E.g.*, *United States v. Cheshire*, 569 F.2d 887, 889 (5th Cir. 1978).

2012 note. Read the guidance in the January 23, 2012 Appellate Section

Report re *United States v. Jones*, 2012 WL 171117 (U.S. Jan. 23, 2012). ("[P]rosecutors should promptly seek warrants for the continued use of any existing and future GPS devices that are or will be attached to vehicles.") Any questions? Contact Mark Eckenwiler at OEO.

Should a search warrant under Rule 41 of the Federal Rules of Criminal Procedure be sought, a court, under 18 U.S.C. § 3117, may issue a warrant authorizing the use of a tracking device both within and outside the court's jurisdiction, as long as the device is installed in the court's jurisdiction. 18 U.S.C. § 3117; *United States v. Gbemisola*, 225 F.3d 753, 758 (D.C. Cir. 2000). Rule 41 sets forth specific requirements for the service and return of search warrants applied to tracking devices. The officer executing the warrant is required to note on the warrant the time and date that the device is installed. Fed. R. Crim. P. 41(f)(2)(A). The officer is then required to return the warrant to the court and serve the warrant upon the person tracked, or person who owns the vehicle tracked, within ten calendar days of when the officer has ceased using the device. Fed. R. Crim. P. 41(f)(2)(B), (C). Rule 41(f)(3), in conjunction with 18 U.S.C. § 3103a(b), allows the delay of notice upon motion by the government.

3.8

Cellular telephone location information

westlaw query celll +1 phone telephone /p location /p 2703

Cellular telephones operate by transmitting and receiving signals to and from towers maintained by telecommunications service providers. When a cellular telephone is powered on, it constantly scans for the strongest signal emitted by a cellular tower, which is typically the closest tower geographically to the telephone. The cell phone then re-scans approximately every seven seconds. When the telephone locates a cellular tower, it sends registration information to the tower, which is the technical means by which a provider identifies a subscriber, validates the account, and routes call traffic. Telecommunications providers, therefore, are capable of determining the approximate physical locations of their customers's telephones based on the physical locations of the cellular towers with which the telephones have registered. The efficacy of the tower, or "cell-site," information varies based on the user's geographic location. In New York City, for example, cellular towers might be several hundred feet apart, allowing for a more precise determination of the telephone's location. In rural areas, on the other hand, the cellular towers often are many miles apart and only indicate a broad geographic area where a cellular phone user might be located.

Telecommunications providers can, however, determine with greater accuracy the physical location of a cellular telephone through a multilateration process. By measuring signals from more than one tower simultaneously upon special request, providers can determine a more precise location of the telephone. Multilateration data can provide for real time monitoring of a telephone's location, or providers may record cellular tower information to provide historical monitoring of the telephone's location.

Most telephones manufactured today also have GPS capability. Cellular telephones with GPS capability are capable of obtaining their own location information from satellite constellations. Generally, GPS-generated location information, while often accessible to service providers, is not transmitted routinely to the service provider. The Federal Communications Commission requires that telecommunications providers be able to locate a percentage of their call participants, as provided in 47 C.F.R. § 20.18(h)(1)(i), (ii).

Law enforcement agents have sought to use the location-monitoring capability of cellular technology to determine the physical location and movements of illegal drug traffickers. Such efforts have involved non-multilaterated or "prospective" cell-site information, historical cell-site data, multilaterated cell-site information, or GPS data. OEO has recommended that prospective cell-site information be sought by combining pen register authority under 18 U.S.C. § 3121-27 with 18 U.S.C. § 2703, which

provides for the disclosure of stored cellular telephone subscriber information by service providers. This "hybrid" approach requires a recitation of specific and articulable facts showing that the information sought is relevant and material to an ongoing criminal investigation. The hybrid approach, however, has been met with mixed success. Compare *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) (allowing government to obtain cell site information consisting of the tower receiving transmissions from target phone), and *In Matter of Application of U.S. for an Order*, 411 F.Supp.2d 678, 682 (W.D. La. 2006) (allowing government to obtain cell site information), with *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*, 402 F.Supp.2d 597, 604-05 (D. Md. 2005) (holding that government could not obtain cell site data under §§ 3122 and 2703); *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, 139 (D.D.C. 2006) (requiring government to show probable cause in order to obtain cell site information); *In re Application for Pen Register and Trap/Trace Device with Cell Site Location*, 396 F.Supp.2d 747, 764 (S.D. Tex. 2005) (holding that government cannot obtain prospective cell site data because such data was analogous to a tracking device).

For multilaterated cell-site information or GPS data, OEO recommends that a search warrant be sought under Rule 41 of the Federal Rules of Criminal Procedure. Further OEO guidance may be found in DOJNet at <http://dojnet.doj.gov/usao/eousa/ole/usabook/cell/01cell.htm>.

Practice note. If authority for GPS, multilaterated cell-site, or other form of location data via cellular telephone is requested and granted under Rule 41 as part of a Title III order authorizing electronic surveillance, and the authorization is subsequently exercised to monitor the location of the telephone electronically, the return requirements of Rule 41 should apply. In seeking delayed notification of the targets of the Title III investigation, attorneys should also request delayed notification under Rule 41.

3.9

Consensual monitoring

westlaw query 18 +s 2511(2)(c)

One exception to the Title III prohibition against the interception of oral, wire, or electronic communications by law enforcement agents is consensual monitoring, where one party to a communication gives prior consent for the interception to law enforcement agents. Such interception may occur through the use of hidden recording devices that capture oral communications, telephone calls recorded with the consent of a cooperating informant who is a party to the communication, or through Internet communications associated with "listservs" or chat rooms, where access to the communications is generally available to the public.

Authorization for such interception is specifically provided in 18 U.S.C. § 2511(2)(c): "It 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." Thus, when a law enforcement officer or government informant is a participant in a conversation and records the conversation, the recording is admissible in court.

Apart from legislative authority, the Supreme Court has long recognized consensual monitoring as a legitimate law enforcement tool. The Court has observed that, since an undercover agent or informant could write down the conversation with a suspect and later testify about the conversation, the Fourth Amendment did not require a different result "if the agent instead of immediately reporting and transcribing his conversations with [the 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), or (2) carries radio equipment which simultaneously transmits the conversations either to recording equipment located elsewhere or to other agents monitoring the transmitting frequency." *United States v. White*, 401 U.S. 745, 751 (1971); accord *United States v. Caceres*, 440 U.S. 741, 757 (1979).

Practice note. Statements intentionally elicited after the Sixth Amendment has attached may violate a target's right to counsel. See the cases surveyed in *Federal Confessions Law* Chapter 7, on DOJNet at <http://dojnet.doj.gov/usao/eousa/ole/usabook/fcon/07fcon.htm>.

Situations may arise where the cooperating informant is unavailable at trial or the prosecutor makes the tactical decision not to call the informant to testify. Consensual tape recordings containing conversations between a defendant and an informant or any other unavailable witness may still be admissible, assuming that the predicate for the admission of the tape recordings can be satisfied. Fed. Rule Evid. 901(b)(5). The defendant's statements on the tape are admissible under the Federal Rules of Evidence 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 that the defendant has adopted or manifested a belief in their truth under Rule 801(d)(2)(B), or for the limited purpose of putting the defendant's responses in context and making those responses intelligible to the jury. *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 would not be 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 does not apply. *United States v. McClain*, 934 F.2d 822, 832 (7th Cir. 1991); *Gutierrez-Chavez*, 842 F.2d at 81 (finding no violation of Confrontation Clause where only incriminating statements of informant to be taken as true were those statements which, in judgment of jury, were adopted by defendant.)

Practice note. By offering the informant's statements in this fashion, the government removes the informant as its "witness." *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. Prosecutors may 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 Federal Rule of Evidence 806 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). *McClain*, 934 F.2d at 833 (holding that Rule 806 does not apply to adopted statements under Rule 801(d)(2)(B)).

Practice note. When a cooperating defendant 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 DOJNet at <http://dojnet.doj.gov/usao/eousa/ole/usabook/drug/forms/401.htm>.

Practice note. Consensual monitoring of oral communications may be accomplished by placing microcassettes, digital recording devices, or small wireless transmitters on cooperators. A problem associated with hidden transmitters is that receivers, typically located in an agent's vehicle, must be

located close enough to the transmitter to detect the communications. The problem may be overcome either by using transmitter devices that send signals via cellular telephone towers or by using digital recording devices with extended memory capacities.

Practice note. Consensual monitoring of wire communications may be accomplished either through the direct recording of conversations by agents or through court order served on a service provider. Such court orders, which do not require OEO review or approval, may be preferable in cases where an informant is traveling with a suspect. When such orders are used, monitors of the intercepted conversations should be familiar with the informant's voice so that they can minimize an interception if they do not hear the informant's voice during the conversation. Forms for the application, order and written consent appear as Forms 302, 303, and 304 on DOJNet at <http://dojnet.doj.gov/usao/eousa/ole/usabook/drug/forms>.

3.10

Video surveillance

Law enforcement agents often employ stationary pole cameras and other forms of electronic video surveillance to monitor activity in a location believed to be used to facilitate illegal drug trafficking or money laundering. The cameras are typically placed in front of a house, apartment or business, in areas readily accessible to the public. Because drug traffickers lack a reasonable expectation of privacy in public areas, no judicial authorization is required for the placement of such cameras. *E.g.*, *United States v. Jackson*, 213 F.3d 1269, 1280-81 (10th Cir. 2000) (judgment vacated on other grounds). Courts have found an expectation of privacy in a hotel room, *United States v. Nerber*, 222 F.3d 597, 604 (9th Cir. 2000); a private backyard where a surveillance camera had been placed on a telephone pole, *United States v. Cuevas-Sanchez*, 821 F.2d 248, 251 (5th Cir. 1987); and an office, *United States v. Taketa*, 923 F.2d 665, 677 (9th Cir. 1991).

As with consensual monitoring of oral communications, an informant or undercover agent also may consent to the videotaping of a meeting or conversation with a hidden camera in an otherwise private location. *United States v. Corona-Chavez*, 328 F.3d 974, 981 (8th Cir. 2003); *United States v. Laetividal-Gonzalez*, 939 F.2d 1455, 1460 (11th Cir. 1991).

If agents seek to conduct video surveillance in a place where a suspect would maintain a reasonable expectation of privacy, the agents must obtain a search warrant under Rule 41 of the Federal Rules of Criminal Procedure. The requirements for obtaining Rule 41 authority to videotape surreptitiously a private location, while non-statutory, are nevertheless similar to Title III requirements set forth in 18 U.S.C. §§ 2510-2522. Courts generally have required that:

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*); see *United States v. Mesa-Rincon*, 911 F.2d 1433, 1437 (10th Cir. 1990) (adding fifth requirement of probable cause to believe that particular person is committing, has committed or is about to commit, crime).

The Department also requires that any application for video surveillance include a particularized description of the premises and names of persons to be surveilled, if known. USAM 9-7.230. Prior to applying to a court for authorization 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. Applications should be submitted through OEO.

Since the basis for installing and monitoring a hidden video camera is Rule 41, 18 U.S.C. § 3103a(b), governing delayed notice, applies. Forms 23 and 24 in the *Electronic Surveillance Manual*, at <http://dojnet.doj.gov/usao/eousa/ole/usabook/elsu/20elsu.htm>, and 326-327 on DOJNet at <http://dojnet.doj.gov/usao/eousa/ole/usabook/drug/forms>, have been revised to include delayed notice language.

3.11

Other electronically-enhanced surveillance techniques

westlaw query Kyllo "thermal imaging" /p "Fourth Amendment"

Other forms of electronically-enhanced surveillance include thermal imaging, artificial illumination, and aerial surveillance.

Occasionally used in marijuana growing and harvesting investigations, thermal imaging involves employing a device—often from an airplane—that measures heat radiation. The radiation may come from a house or other structure on a suspect's property. An inordinate amount of heat being radiated may indicate the use of indoor lights associated with marijuana cultivation, and such information may be incorporated into a search warrant for the property.

In *Kyllo v. United States*, 533 U.S. 27, 34-35 (2001), the Supreme Court held 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.* at 40. Thus, agents must obtain search warrants before using a thermal imaging device.

A thermal imaging device may still be used to survey the curtilage of a house or commercial structure without a search warrant. If the device is used from an aircraft, the aircraft should be in public airspace and comply with Federal Aviation Administration regulations regarding altitude. See *California v. Ciraolo*, 476 U.S. 207, 225 (1986) (holding that overflight of individual's backyard from airplane lawfully operated does not violate the Fourth Amendment); *Dow Chemical Co. v. United States*, 476 U.S. 227, 229 (1986) (holding that overflight of industrial complex from airplane lawfully operating does not violate the Fourth Amendment).

The use of artificial technology to illuminate areas otherwise open to the plain view of law enforcement does not implicate constitutional concerns. The Supreme Court held in *Texas v. Brown*, 460 U.S. 730 (1983), that "the use of artificial means to illuminate a darkened area simply does not constitute a search." *Id.* at 773-74. While *Brown* involved

a police officer shining a flashlight into a vehicle, the Court has held similarly in the context of a flashlight directed inside a darkened barn, *United States v. Dunn*, 480 U.S. 294, 304-05 (1987), or on the deck of a ship, *United States v. Lee*, 274 U.S. 559, 563 (1927).