



U.S. Department of Justice

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

Requester: Catherine Crump Request Number: 07-4123

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

SEP -8 2008

Dear Requester:

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

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

Enclosed please find:

- 13 page(s) are being released in full (RIF);
- 1 page(s) are being released in part (RIP);
- 161 page(s) are withheld in full (WIF). **The redacted/withheld documents were reviewed to determine if any information could be segregated for release.**

The exemption(s) cited for withholding records or portions of records are marked below. An enclosure to this letter explains the exemptions in more detail.

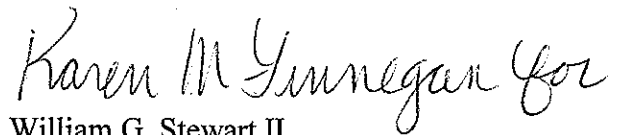
Section 552

Section 552a

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

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

Sincerely,

A handwritten signature in cursive script that reads "Karen M. Gunnegan for".

William G. Stewart II
Assistant Director

Enclosure(s)

Requester: Catherine Crump
FOIA #: 07-4123

Continuation Sheet:

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

This response is to FOIA No. 07-4123 only and does not include search results associated with the other requests listed above.

EXPLANATION OF EXEMPTIONS

FOIA: TITLE 5, UNITED STATES CODE, SECTION 552

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

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

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

Memorandum



Subj: Government's Position Regarding Magistrate Judge Orenstein's Decision Requiring Warrants for Cell Site Location Information	Date: September 13, 2005
--	-----------------------------

To: Robert M. Block
Chief United States Magistrate Judge
Central District of California

From: AUSA Lisa E. Feldman
AUSA Brian M. Hoffstadt

Last month, you forwarded to our Office the Memorandum and Order authored by Magistrate Judge James Orenstein (E.D.N.Y.), in which Judge Orenstein held that the government could not obtain "cell site / sector (physical address)" data from cellular telephone companies without a warrant supported by probable cause. Given that the practice in this District has been to obtain this type of data through an order demonstrating "specific and articulable facts" under 18 U.S.C. § 2703(d) -- rather than through a warrant -- you requested our input regarding whether the opinion is sufficiently sound that it should be followed in this District as well.

We appreciate this opportunity to provide our views to you. As set forth in summary form below (and in a letter brief filed with Judge Orenstein by the U.S. Attorney's Office in the Eastern District of New York as well as a longer, attached memorandum authored by Chuck Rosenberg, the United States Attorney in the Southern District of Texas), we believe that Judge Orenstein's opinion is not consistent with the relevant statutory provisions. To the contrary, § 2703(d) -- either on its own or read in conjunction with the pen register statutes, 18 U.S.C. § 3121 *et seq.* -- authorizes the government to obtain "cell site / sector (physical address)" data from cellular telephone companies with a § 2703(d) order.

In his opinion, Judge Orenstein finds that the government may compel a cellular telephone company to disclose "the location of cell site / sector (physical address)" data -- that is, information indicating which cell towers a particular cellular telephone is using -- only if it obtains a warrant supported by probable cause. In reaching this conclusion, Judge Orenstein reasons that neither 18 U.S.C. § 2703(d) nor the pen register / trap-and-trace statutes authorize disclosure of this information. Judge Orenstein first reasons that § 2703(d) does not permit the government to obtain cell site location data because (i) 18 U.S.C. § 2703(c)(1)(B) and § 2703(d) authorize disclosure of "the contents of a wire or electronic communication"; (ii) the definition of "electronic communication" in 18 U.S.C. § 2510(12) specifically excludes "tracking devices"; (iii) a cell phone is a "tracking device" because it is, under 18 U.S.C. § 3117(b), "an electronic or

RIF

mechanical device which permits the tracking of the movement of a person or object"; (iv) cell site location information is accordingly not "the contents of a wire or electronic communication" and therefore falls outside the statutory reach of a § 2703(d) order. Judge Orenstein further finds that the pen register and trap-and-trace statutes, 18 U.S.C. § 3121 *et seq.* do not provide authority for cell sector location data, notwithstanding the fact that such data falls within the scope of a "pen register" and "trap and trace device" as defined in the post-PATRIOT Act amendments to 18 U.S.C. §§ 3127(e), 3127(f), because 42 U.S.C. § 1002(a)(2)(B) specifically prohibits telecommunications carriers from disclosing "any information that may disclose the physical location of the subscriber . . ." Due to the absence of either basis of statutory authority, Judge Orenstein concludes that a warrant supported by probable cause is necessary.

The reasoning of this decision is flawed for several reasons.

First, the plain language of 18 U.S.C. § 2703 authorizes the government to obtain, from cellular telephone companies and others, cell site location data. As part of the Electronic Communications Privacy Act ("EPCA"), § 2703 requires the government to use three different levels of process depending on what type of information it seeks to obtain from any "provider of electronic communication service." At one end, the government may obtain certain basic subscriber records (*i.e.*, name, address, call-in numbers, session duration, length of service, source of payment) with a subpoena. *See* § 2703(c)(2). At the other end, the government may obtain the "contents of a wire or electronic communication," but only with a search warrant. *See* § 2703(b)(1)(A), 2703(a). Between these two extremes is any "record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications)"; to obtain any of this non-content information, the government must obtain from the court an order pursuant to § 2703(d), which requires the government to demonstrate an intermediate level of cause -- namely, that "specific and articulable facts show[] that there are reasonable grounds to believe that . . . the records or information sought . . . are relevant and material to an ongoing criminal investigation." *See* § 2703(d). Because cell site location data is not "content" but lies outside the universe of basic subscriber records that may be obtained by subpoena, such information falls within the intermediate level of records for which the government must obtain a § 2703(d) order.

Judge Orenstein's analysis parses this statutory language incorrectly. In his analysis, Judge Orenstein asks whether cell phone information fits within the definition of the "contents of a wire or electronic communication" (and goes on to conclude that cell site location information falls outside the definition of an "electronic communication"). This is the wrong question, however. The government, when it requests cell site location data, is not seeking the "contents of a wire or electronic communication"; rather, it is seeking a "record or other information." (The language regarding "contents of a wire or electronic communication" is contained in § 2703(d) because the usual rule requiring a warrant for "contents," *see supra*, is relaxed if the government gives prior notification, *see* § 2703(b)(1)(B)). Cell site data falls squarely within the definition of a "record or other information pertaining to a subscriber to or customer of [the cell phone

company]" under § 2703's three-tiered scheme.¹

Thus, the legitimate use of § 2703(d) to obtain cell site information hinges on whether the government can require the disclosure of that information -- that is, the "record or other information pertaining to a subscriber to or customer of [the cell phone company]" -- under § 2703(c)(1). See § 2703(d) (making § 2703(d) orders applicable for disclosures pursuant to "subsection (b) or (c)"). Section 2703(c)(1) empowers the government to "require a provider of electronic communication service . . . to disclose a record or other information pertaining to a subscriber to or customer of [the cell phone company]." (Emphasis added). An "electronic communication service" means "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15) (emphasis added). A "wire communication" is "any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection." *Id.* § 2510(1). Wireless, cellular telephone conversations fit within this statutory definition, as "aural transfer[s]" using "facilities for the transmission of communications by the aid of . . . other like connection[s]." ECPA's legislative history explicitly confirms this reading. See S. Rep. No. 541, 99th Cong., 2d Sess., at 11 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3565 ("cellular communications . . . are included in the definition of 'wire communications'"); H.R. Rep. No. 647, 99th Cong., 2d Sess., at 31 (1986) (noting that "the Committee intends that 'wire communication' be construed to include communications made over cellular systems"). As a result, cell phones constitute an "electronic communications service" because they "provide the ability to send or receive wire communications"; the companies that provide cell phones are "provider[s] of electronic communication service"; thus, those companies may be required to disclose cell site location data under § 2703(c)(1).²

Under the analysis set forth above, whether a cell phone is a "tracking device"-- a linchpin of Judge Orenstein's opinion -- is never reached, and accordingly does not bear on the proper use of § 2703(d) to obtain cell site location information. The term "tracking device" was relevant to Judge Orenstein's decision solely because he was trying to determine whether a cell phone fell within the definition of "electronic communication" under 18 U.S.C. § 2510(12). As the analysis in this memorandum demonstrates, however, the definition of "electronic

¹ Moreover, cell site location information falls outside the definition of "contents," which is defined as "the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8).

² Though not addressed by Judge Orenstein's opinion, § 2703 also seems to contemplate the disclosure of cell site location data on an ongoing basis. The text of § 2703(c) authorizes disclosure of "records or other information pertaining to a subscriber or customer" but does not require that those records be in existence at the time the § 2703(d) order is issued. More to the point, this type of ongoing, non-content information has long been acceptably obtained through pen registers and trap-and-trace orders; because § 2703(d) requires a greater showing of cause than the pen register and trap-and-trace orders, the government is being more solicitous of individual privacy by seeking authorization under § 2703(d).

communication" is never confronted because §§ 2703(c)(1) and (d) expressly provide that "providers of electronic communications services" -- which includes the "wire communications" transmitted over cell phones -- may be compelled to disclose cell site location data with a § 2703(d) order.

Even assuming that it were somehow relevant whether a cell phone is a "tracking device," Judge Orenstein's analysis on this point is flawed as well. As noted above, § 3117 defines a "tracking device" solely as "an electronic or mechanical device which permits the tracking of the movement of a person or object." 18 U.S.C. § 3117(b). According to ECPA's legislative history, this term was meant to reach "homing devices" -- that is, "one-way radio communications devices that emit a signal on a specific radio frequency." S. Rep. No. 541, at 10, reprinted in 1986 U.S.C.C.A.N. at 3564. A cell phone is not a "homing device" because cell site location data is obtained from transmissions from the cell towers -- not the phone -- and, further, because those towers provide only limited geographic data and do not pinpoint the cell phone's precise location as a "homing device" would. There is also good reason not to take a broader view of the definition of "tracking device" under § 3117(b). Section 3117 is a statute concerned with territorial venue, not with the question presented here. See § 3117(a) (discussing how device installed in one district can be tracked into a different district). Moreover, defining "tracking device" to reach all devices from which one's location could be gleaned -- as Judge Orenstein's opinion does -- has several adverse consequences. Under such a definition, computers connected to the Internet and even land-line phones could be considered "tracking devices" because it is possible to determine one's location from the Internet protocol ("IP") address or telephone number. It is doubtful that Congress intended to create such a large exception to the universe of "electronic communications" through a definition contained in a venue provision.

For these reasons, § 2703 provides an adequate and independent statutory basis for obtaining cell site location information through a § 2703(d) order.

Second, and alternatively, the government is authorized to obtain cell site location data by relying in part upon the pen register and trap-and-trace statutes -- when they are read in conjunction with § 2703(d). Cell site location data falls within the reach of the pen register and trap-and-trace statutes because those statutes, since the enactment of the PATRIOT Act, have authorized the capture of "dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire . . . communication is transmitted . . ." 18 U.S.C. §§ 3127(3) (pen register definition), 3127(4) (trap and trace device definition). The government recognizes that Congress had, in 1994, prohibited telecommunications carriers from disclosing, through a pen register or trap-and-trace order, "any information that may disclose the physical location of the subscriber." 47 U.S.C. § 1002(a)(2)(B). The PATRIOT Act amendments ostensibly supersede the earlier 1994 limitations on the use of pen registers or trap-and-trace orders. However, to the extent that the 1994 language retains its force and effect, it at most prevents the government from relying solely on a pen register or trap-and-trace order to obtain cell site information. The government believes that these statutes, at least in conjunction with § 2703, still authorize the release of cell site location data.

Lastly, Judge Orenstein errs in concluding that a warrant supported by probable cause is required if neither § 2703(d) nor the pen register / trap-and-trace device statutes provide express statutory authority to obtain cell site location data. In the absence of extra-constitutional protection granted by statute, the probable cause and warrant requirements come into play only when a "search" or "seizure" occurs within the meaning of the Fourth Amendment. It is well settled, however, that a person has no legitimate expectation of privacy in his physical location in and about public places. See United States v. Knotts, 460 U.S. 276 (1983); cf. United States v. Karo, 468 U.S. 705 (1984). Given the limited information that cell site location data typically provides (within several hundred yards), this data does not divulge information about activities inside a particular private residence. Moreover, a person's actions in using a cell phone automatically disclose his location to the cell phone provider, and such disclosures to third parties also falls outside any legitimate expectation of privacy. See United States v. Miller, 425 U.S. 435 (1976) (no "search" when government obtains bank records disclosed to third-party banks by virtue of banking system); Smith v. Maryland, 442 U.S. 735 (1979) (no "search" when government obtains toll records disclosed to telephone company by virtue of use of phone). Because cell site location data ostensibly falls outside the scope of the Fourth Amendment, if Judge Orenstein is correct that this data falls outside of § 2703 and the pen register / trap-and-trace statutes, that data is ostensibly available by subpoena alone. That is not the result the government seeks, however. Cell site location data is entitled to at least as much privacy protection as basic subscriber information, which is why the government believes that § 2703(d) -- and its requirement of "specific and articulable facts" -- provides the proper pre-requisite to obtaining this data.

In sum, § 2703(d) -- both alone and in conjunction with the pen register / trap-and-trace statutes -- provides ample authority upon which to obtain cell site location data from cell phone companies. By requiring the government to make a showing of "specific and articulable facts" before obtaining this data, Congress has properly balanced the privacy interests of individuals with the needs of law enforcement. Imposing a warrant requirement, as Judge Orenstein suggests, is neither required by the statutes he cites nor by the Fourth Amendment.

Enclosures:

- o Letter Brief to United States Magistrate Judge James Orenstein (prepared by U.S. Attorney's Office, Eastern District of New York)
- o Memorandum of Law to United States Magistrate Judge Stephen William Smith (prepared by U.S. Attorney's Office, Southern District of Texas)

Wilkison, Tracy (USACAC)

From: Robert_Block@cacd.uscourts.gov
Sent: Tuesday, July 10, 2007 2:15 PM
To: Wilkison, Tracy (USACAC)
Cc: Steve Hillman
Subject: RE: applications for cell site and GPS information

Good. Thanks.

"Wilkison, Tracy (USACAC)" <tracy.wilkison@usdoj.gov>

07/10/2007 02:13 PM

To <Robert_Block@cacd.uscourts.gov>
cc
Subject RE: applications for cell site and GPS information

That is true. As far as I'm aware, no one has yet filed one of the new applications - when they do, they are to email it to (now) Dan Goodman, and he will forward to Judge Walsh.

From: Robert_Block@cacd.uscourts.gov [mailto:Robert_Block@cacd.uscourts.gov]
Sent: Tuesday, July 10, 2007 2:10 PM
To: Wilkison, Tracy (USACAC)
Subject: RE: applications for cell site and GPS information

Thanks. As I recall, at the meeting you said that when you started using the new forms you were going to forward copies of filed applications to Judge Walsh.

"Wilkison, Tracy (USACAC)" <tracy.wilkison@usdoj.gov>

07/10/2007 02:08 PM

To <Robert_Block@cacd.uscourts.gov>
cc
Subject RE: applications for cell site and GPS information

Judge Block,
We have just started to use the new forms. They should be the only forms you see from now on.

Today is my last day before beginning maternity leave. If you have any questions on this or related issues, please contact Dan Goodman at 894-4667.

Thanks,
Tracy Wilkison

From: Robert_Block@cacd.uscourts.gov [mailto:Robert_Block@cacd.uscourts.gov]
Sent: Tuesday, July 10, 2007 1:35 PM

To: Wikison, Tracy (USACAC)

Subject: applications for cell site and GPS information

Tracy, at today's Magistrate Judges meeting, I was asked to inquire of you when the Govt planned to start using the new application forms that were discussed at our June 6 meeting.

Wilkison, Tracy (USACAC)

From: Kowal, David (USACAC)
Sent: Wednesday, June 25, 2008 3:44 PM
To: USACAC-AUSAs Criminal
Subject: New Form - GPS / Cell Site Return - S:\Criminal Forms\Pen Registers\Cell Site and GPS apps

I've said it before - no event brings the Criminal Division together like the posting of a new form on the S:drive.

With this in mind, your Investigative Technology Coordinators and Dept. Criminal Chief Daniel Goodman proudly announce the creation of a new form for returns on orders for real time GPS or cell site monitoring.

The new form, to be filled out by the AUSA and sworn out by the agent before the duty mag. judge, is located at **S:\Criminal Forms\Pen Registers\Cell Site and GPS apps** with the rest of the cell site and GPS forms. (Please recall that an updated directory of common investigatory forms is kept at **S:\Criminal Forms** under the name "DIRECTORY OF FORMS").

As you may know, the magistrate court bench requires us to comply with Rule 41 procedures in order to obtain orders for real time monitoring of phones using GPS technology at any time, or using cell site information without limitation as to whether the phone is making a call. For such orders we must do a return similar to that for a tracking device, though one less burdensome than the inventory and return required for a common property search warrant. As the magistrate judges have also recently asked us to standardize our returns for these orders, please use this new form for your cases if at all possible. Please also note that no return is required on orders for purely historical cell site info or orders authorizing cell site information solely when a call is made, for such orders are not authorized under Rule 41.

In keeping with office policy on all forms concerning telephones, this new form contains a bewildering series of fill-in-the-blank options depending on whether you're listing the relevant information yourself or just attaching a log already prepared by the agent. The form also reflects such radical policy choices as the use of Times New Roman font to save space, and contains options for under seal filing.

If you have any comments, suggestions, or otherwise wish to join me in announcing yourself to the office as a nerdy loser who spends time working on forms, please contact Erik Silber, Tracy Wilkison, or me. If your comment concerns a legal issue or is otherwise substantive, try Erik or Tracy. If it pertains to font choice or formatting, I'm your man.

Thanks

ps: Please note the reduced font size and dual color (including the always classy Yale blue) in my already much-imitated signature block

David P. Kowal
Assistant United States Attorney
United States Courthouse, Suite 1400 | 312 N. Spring St. | Los Angeles, California 90012
T: 213.894.5136 | F: 213.894.0142 |

Wilkison, Tracy (USACAC)

From: Wilkison, Tracy (USACAC)
Sent: Monday, July 28, 2008 5:43 PM
To: USACAC-AUSAs Criminal
Subject: changes to GPS/ cell site for investigations form.

Hi all,

Following what can only be described as a Santa Ana Judicial Revolt, some changes have been made to the GPS/ Cell site form. Note that the changes ONLY apply if you are **seeking this information during an investigation**, and you are **seeking GPS info, or cell site info whenever the phone is turned on**. If both of those things are true, you will be following the procedures of Rule 41, and you MUST use the new and improved form. The changes are procedural, more than substantive.

The biggest changes (ONLY APPLICABLE WHEN YOU ARE FOLLOWING THE PROCEDURES OF RULE 41):

1. The "proposed order" accompanying the application will now be titled "[proposed] Warrant." References to "order" throughout also have changed.
2. The warrant now requires that any applications for continued delayed notice, and the eventual return, be made to the judge that signed the original Warrant, unless directed otherwise by that court. This is different from how we handle this in virtually every other situation, so please note this.
3. **Signing and Returns: THIS IS REALLY DIFFERENT:** When the cell site/GPS Warrant is signed by a judge, the agent will retain the original of the Warrant, as he/she would for search warrants (it won't get filed, although it does get a number assigned to it). When it is time for the Warrant to be returned, you will fill out a return form (also on the S:drive), with the necessary information included. You will then attach this to the original Warrant. The agent will then return the warrant to the same judge that issued the warrant, and thereafter, the entire warrant and return will be filed.
4. If you ask to seal the warrant and the return in your initial request to seal, you won't have to do one again at the end.

Attached are the forms, also available at S:\Criminal Forms\Pen Registers\Cell site and GPS Apps



cell site and GPS
investigatio...



GPS & Cell Site
Return Form (0...

Wilkison, Tracy (USACAC)

From: Goodman, Daniel (USACAC)
Sent: Thursday, October 26, 2006 9:33 AM
To: Fitzgerald, Patrick (USACAC); Duarte, Elena (USACAC); Wilkison, Tracy (USACAC); Murphy, Cheryl (USACAC); Castro-Silva, Rodrigo (USACAC)
Cc: Feldman, Lisa; Terrell, Mike (USACAC); Villeza, Rob (USACAC); Donahue, Patricia (USACAC); Kin, Curtis (USACAC)
Subject: Prospective Cell Site Information
Importance: High

Attached is a draft of a letter about cell site applications that in my opinion is appropriate to send to Chief Magistrate Judge Zarefsky. (I need to check the address to make sure I have it right.) Please let me know what you think at your earliest convenience.



cellsitelet_zar.wpd

Wilkison, Tracy (USACAC)

From: Duarte, Elena (USACAC)
Sent: Thursday, November 30, 2006 11:49 AM
To: Goodman, Daniel (USACAC); Wilkison, Tracy (USACAC)

NY weighs in . . . My contact from EDCA is out so I'll call her.



RE: cell phone GPS location in... RE: GPS location info

RIE

Wilkison, Tracy (USACAC)

From: Demarco, Joseph (USANYS)
Sent: Thursday, November 30, 2006 10:44 AM
To: Duarte, Elena (USACAC)
Subject: RE: GPS location info
Attachments: onstarord2.wpd; onstar2.wpd; onstaraff2.wpd

Here is what I believe is our current sample the On-Star flavor, at least.

Joe.

-----Original Message-----

From: Duarte, Elena (USACAC)
Sent: Thursday, November 30, 2006 1:03 PM
To: Demarco, Joseph (USANYS)
Subject: FW: GPS location info

What type of authority/order are you guys currently using to get GPS info off cell-phones?

Wilkison, Tracy (USACAC)

From: Robert_Block@caed.uscourts.gov
Sent: Thursday, June 21, 2007 2:30 PM
To: Wilkison, Tracy (USACAC)
Subject: proposed orders for cell site and GPS information

Tracy, we've reviewed your proposed orders, and here are our comments.

1. It's difficult for us to evaluate the proposed orders outside the context of the applications.
2. The proposed order for historical cell site information looks okay.
3. Assuming we agree that the All Writs Act provides the requisite authority, the proposed order for prospective cell site [and gps] information in a fugitive case also looks okay, except that we think the words "federal crimes or" should be eliminated from the court findings paragraph.
4. We do have some problems with the proposed order for prospective cell site [and gps] information in an ongoing investigation because it seems to us that there should be two versions: one version for situations where the judge will not be requiring compliance with the Rule 41 procedures for tracking device warrants, and one version for situations where the judge will be requiring compliance with those procedures. In this regard, we note that the judges are not of the same mind when it comes to the issue of whether or when the Government will be required to comply with the Rule 41 procedures for tracking device warrants. For example, some of the judges may agree with the Government that cell site information always qualifies as stored information, and that it is never necessary for the Government to comply with the Rule 41 procedures for tracking device warrants. We anticipate that many of the judges will take the position that we discussed with you at the meeting (i.e., that compliance with the Rule 41 procedures only is required when the Government is seeking information outside of the progress of a call). However, some of the judges may take the position that, even if the Government only is requesting prospective cell site information for calls actually made and received, if the request is not also limited to cell site information at the beginning and the end of the call, but includes cell site information "if reasonably available, during the progress of the call," the Government is asking for more than the Government applied for or got in those New York cases and consequently will have to follow the Rule 41 procedures for tracking device warrants.

RIE

3. LOCATION TRACKING AND MONITORING

a. TRACKING TELEPHONES - CELL SITE INFORMATION AND GPS TRACKING:

S:\Criminal Forms\Pen Registers\Cell Site and GPS apps

- (1) 1 form for historical cell site info only. (no affidavit needed)
- (2) 2 forms for obtaining real-time info: fugitive/non-fugitive
- (3) Real-time info requires PC based on agent affidavit
- (4) Real-time info also requires use of pre-made affidavits on technical issues which are in folder. See instructions at top of forms.

b. OTHER TRACKING DEVICES - CARS, BEEPERS, ETC.:



non-responsive

c. POLE CAMERA:



non-responsive

4. WIRETAPS

a. TELEPHONES



non-responsive

b. E-MAIL, ISP'S, WEB SITES ETC.



non-responsive

5. MISC.

a. TELEPHONES: REVERSE NUMBER SEARCH



non-responsive

RIP

N/A