USABook > Electronic Surveillance > Cell Site Simulators, Triggerfish, Cell Phones

A cell site simulator (sometimes called a digital analyzer, cell site locator, triggerfish, ESN reader, or swamp box) is a mobile device that can electronically force a cell phone to register its telephone number (MIN), electronic serial number (ESN), and information about its location, when the phone is turned on. This can be done without the user knowing about it, and without involving the cell phone provider.

Section 216 of the Patriot Act altered the definition of a pen register in 18 U.S.C. § 3127 (3) so that it includes these devices. Consequently, a pen register/trap and trace order must be obtained by the government before it uses such a device.

The use of a triggerfish to locate cellular telephones is an issue of some controversy. The Office of Enforcement Operations (OEO) encourages AUSAs to contact Mark Eckenwiler at (202) 616-0435 if they have questions or concerns.

Note. It may also be possible to flash the firmware of a cell phone so that you can intercept conversations using a suspect's cell phone as the bug. You don't even have to have possession of the phone to modify it; the "firmware" is modified wirelessly. This law enforcement tool was recently discussed in a Memorandum Opinion from SDNY, and has been getting a bit of news coverage lately. The authority for doing this can be found in 18 U.S. C. § 2518(11), but it sounds like something that you would not want to do without checking with OEO first.

See also:

- *Electronic Surveillance Manual* Chapter XIV
- Electronic Surveillance Issues
- *Federal Narcotics Prosecutions* § 3.16
- 76 ALR4th 536 ("Search and Seizure of Telephone Company Records Pertaining to Subscriber as Violation of Subscriber's Constitutional Rights")
- USABook topic pages: Electronic Surveillance; Pen Registers

updated 02/23/07

PROCEDURES FOR AUTHORIZING EMERGENCY INSTALLATION OF PEN REGISTER AND TRAP AND TRACE DEVICES ("PEN/TRAP") UNDER 18 U.S.C. 3125

I. **Justification:**

A. A situation where there is: 1) an immediate threat to life or limb; 2) a threat to national security; 3) activity characteristic of organized crime; or 4) an ongoing attack of a protected computer (one used by financial institution or U.S. government) where violation is a felony; AND

B. An order cannot be obtained with an exercise of due diligence, AND

C. There are grounds upon which an order could be issued (information sought is relevant to ongoing criminal activity).

II. **Procedures:**

A. Obtain the following, relevant facts: 1) circumstances giving rise to the emergency situation; 2) who, if known, is using the target phone/facility; 3) how the phone/facility was identified; 4) when the phone/facility was last known to be used; and 5) most recent criminal activity.

B. Call a Deputy Assistant Attorney General (DAAG), through the Command Center, at (b)(6)&(7)(C)

C. Once approval has been obtained, call the law enforcement officer or AUSA back and advise them of the following: 1) an application and order must be filed within 48 hours (weekends and holidays included) after the installation of the equipment has occurred or begins to occur; and 2) the authorization obtained applies only to that specific phone/facility - the use of a pen/trap on any additional phones or facilities that may be identified during the emergency situation need to authorized by the DAAG.

III. **Consent:** If the request pertains to the victim's phone or a phone used by someone who is cooperating with the investigation, consider whether consent would apply. The cooperating party may consent to the installation of a trap and trace/pen register on their phone, and with respect to the victim, consent may be implied depending on the circumstances. See 18 U.S.C. 3121(b)(2)("user" may consent)

PROCEDURES FOR EMERGENCY REQUESTS FOR CELL SITE DATA WHEN SOUGHT IN CONNECTION WITH A PEN/TRAP

I. **Justification:** See above

II. **Procedures:** See above. When advising the AUSA or agent about filing the application and proposed order, instruct them to file an application that cites to both the pen register/trap and trace statute and 18 U.S.C. 2703(d).

III. **Invocation of 18 U.S.C. 2702(c)(4) to receive prospective cell site:** Reliance on this provision to allow repeated, perspective collection of cell site data may be problematic. Judicious use of this provision is advised. Advise the field that the more prudent course of action is to obtain a search warrant under Rule 41 for repeated disclosures of prospective cell site information because Rule 41 has prospective effect.

IV. **Consent:** As with an emergency pen/trap request, consider whether consent would apply. See 18 U.S.C. 2702(c)(2) - allowing a provider to disclose a record or other information with the consent of the "customer or subscriber."

* **NOTE:** A service provider can voluntarily disclose **historical** cell site data under 18 U.S.C. 2702(c)(4), and follow-up compulsory process is unnecessary.

PROCEDURES FOR EMERGENCY REQUESTS FOR LATITUDE/LONGITUDE DATA FOR CELLULAR PHONES, I.E., GPS, E-911, TOWER TRILATERATION

The Department cannot authorize the collection of GPS (latitude/longitude) data, E-911 information, or location information generated through tower trilateration under the emergency pen/trap statute. (Tower trilateration measures the signal strength from multiple cell towers to locate the phone and is relatively accurate.) If law enforcement seeks this information, they need to obtain a search warrant under Rule 41, absent an emergency or voluntary disclosure by the service provider. Again, consent is an option if the target phone belongs to the victim or someone cooperating with the investigation.

When advising the field, ascertain if the service provider can actually produce the information.

* Sprint/Nextel: True GPS

* T-Mobile: Tower trilateration

* Verizon Wireless/Alltel: no GPS, unless the phone is used to call 911. Typically, these providers can only pinpoint the location of a cell phone within the "banana range" from a cell tower.

In addition, GPS data can only be captured when the phone is on and registering with the network. Providers do not maintain historical GPS/E-911 data. One exception is the "kiddie tracker" phone service.

One final consideration is where to obtain the warrant. Obtain the warrant where the phone is reasonably believed to be.

PROCEDURES FOR EMERGENCY WIRETAP REQUESTS
PURSUANT TO 18 U.S.C. 2518(7)

I. Justification:

A. A situation where there is: 1) an immediate threat to life or limb; 2) conspiratorial activity characteristic of organized crime; or 3) conspiratorial activity threatening national security; AND

B. An order cannot be obtained with an exercise of due diligence; AND

C. There are grounds upon which an order could be issued, i.e. probable cause for a predicate offense and/or federal felony (usually not an issue) and legal necessity.

II. Procedures:

A. Obtain the following, relevant facts: 1) circumstances giving rise to the emergency situation; 2) who, if known, is using the target phone/facility/location; 3) how the target phone/facility/location was identified; 4) when the phone/facility/location was last known to be used; 5) most recent criminal activity; and 6) basis for belief that phone/facility/location will be used for communications concerning the crime, i.e. what evidence is there that the perpetrator is acting in concert with others - what communications will be obtained.

B. Call a DAAG, through the Command Center, at (b)(6)&(7)(C) (b)(6)&(7)(C) and advise the official of the facts.

C. Once the DAAG concurs that an emergency situation exists, call the law enforcement officer or AUSA back and advise them of the following: 1) the Criminal Division agrees that an emergency tap may be sought; 2) the law enforcement officer must proceed up his chain of command to seek approval for the emergency tap; and 3) a high-level official of the law enforcement agency (for example, the Assistant Director or Director of the FBI) must contact either the AG, the DAG, or the AAG (Associate Attorney General) to obtain approval to proceed with the emergency tap.

D. Once the tap has been authorized by DOJ, the AUSA must file an application, affidavit, and proposed order within 48 hours after the interception has occurred or begins to occur. (Sample pleadings are available on USABook).

E. The affidavit in support of the emergency must contain only those facts known to the law enforcement officer at the time the emergency authorization was obtained from DOJ.

F. All pleadings must be reviewed by OEO before the AUSA goes to court.

G. Any documentation of the emergency authorization would come from the law enforcement agency and would include the date and time of the authorization, the identity of the authorizing official, and a description of the phone/facility/location that was authorized for interception, i.e., the phone number for the phone, the email address for the internet account, or the physical address of the location. This documentation should be filed with the AUSA's application. OEO/Criminal Division does not provide such documentation as we are not involved directly with the approval process at the AG/DAG/AAG level.

H. Continued surveillance: If the law enforcement agency wants to extend interceptions beyond the first 48-hour period, then:

1. They must seek DAAG authority to do so.

2. The affidavit filed in support of the emergency request may also include a section that provides probable cause to extend the interceptions. The affidavit must clearly differentiate between those facts in support of the emergency and those in support of the extension request.

3. Separate applications and orders should be filed for the emergency and extension requests.

USE OF WITT EQUIPMENT

WITT is a catchall term for equipment that law enforcement can use to locate a cellular phone. It includes devices called Wolfpack, Stingray, and Gossamer. WITT equipment emulates a cell phone tower and can be used to determine which direction the phone is in and how strong the signal is.

If law enforcement seeks to use their WITT equipment to locate a cellular phone, they need to obtain a pen register and trap and trace order for that phone. If they want to use the WITT equipment in an emergency situation, they must obtain DOJ approval first. Consent, for the reasons stated herein, may also apply.

To: (b)(6)&(7)(C)
From: (b)(6)&(7)(C)
Sent: Wed 8/22/2012 1:45:51 PM

Q7: How can law enforcement use its own equipment to obtain location information for a particular wireless device?

A number of investigative agencies have access to specialized equipment, such as directional antennae, that can be used to obtain location information about a particular wireless device, unbeknownst to the device's user and without the involvement of the wireless provider. Such equipment may be used to locate, among other things, cell phones, computers that are accessing open wireless networks, and PC wireless data cards. For more background information about these kinds of devices, see Chapter XIV of the Electronic Surveillance Manual (OEO).

In order to use this type of equipment, law enforcement needs to obtain the appropriate legal process. A search warrant will always be sufficient to authorize the use of this equipment, but other types of legal process may also be available in some situations. For additional guidance about the types of legal process that are available in a specific case, please contact CCIPS (b)(6)&(7)(C)

In certain cases, the equipment described above can also be used to collect identifying information about the mobile device, such as its electronic serial number (ESN). For more information about the authorization required to use the equipment for this purpose, please contact CCIPS (b)(6)&(7)(C) for the latest guidance and go-bys.

http://dojnet.doj.gov/usao/eousa/ole/usabook/elsu/14elsu.htm

XIV. Cell Site Simulators/Digital Analyzers/Triggerfish

A cell site simulator, digital analyzer, or a triggerfish can electronically force a cellular telephone to register its mobile identification number ("MIN," *i.e.*, telephone number) and electronic serial number ("ESN," *i.e.*, the number assigned by the manufacturer of the cellular telephone and programmed into the telephone) when the cellular telephone is turned on. Cell site data (the MIN, the ESN, and the channel and cell site codes identifying the cell location and geographical sub-sector from which the telephone is transmitting) are being transmitted continuously as a necessary aspect of cellular telephone call direction and processing. The necessary signaling data (ESN/MIN, channel/cell site codes) are not dialed or otherwise controlled by the cellular telephone user. Rather, the transmission of the cellular telephone's ESN/MIN to the nearest cell site occurs automatically when the cellular telephone is turned on. This automatic registration

with the nearest cell site is the means by which the cellular service provider connects with and identifies the account, knows where to send calls, and reports constantly to the customer's telephone a read- out regarding the signal power, status and mode.

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

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

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

(b)(6)&(7)(C)

U.S. Department of Justice, Criminal Division

Office of Enforcement Operations, Electronic Surveillance Unit

1301 New York Ave., N.W. , Washington, D.C. 20530

(b)(6)&(7)(C)

(b)(6)&(7)(C)

PROCEDURES FOR AUTHORIZING EMERGENCY INSTALLATION OF PEN REGISTER AND TRAP AND TRACE DEVICES ("PEN/TRAP") UNDER 18 U.S.C. 3125

I. **Justification:**

A. A situation where there is: 1) an immediate threat to life or limb; 2) a threat to national security; 3) activity characteristic of organized crime; or 4) an ongoing attack of a protected computer (one used by financial institution or U.S. government) where violation is a felony; AND

B. An order cannot be obtained with an exercise of due diligence, AND

C. There are grounds upon which an order could be issued (information sought is relevant to ongoing criminal activity).

II. **Procedures:**

A. Obtain the following, relevant facts: 1) circumstances giving rise to the emergency situation; 2) who, if known, is using the target phone/facility; 3) how the phone/facility was identified; 4) when the phone/facility was last known to be used; and 5) most recent criminal activity.

B. Call a Deputy Assistant Attorney General (DAAG), through the Command Center, at (b)(6)&(7)(C)

C. Once approval has been obtained, call the law enforcement officer or AUSA back and advise them of the following: 1) an application and order must be filed within 48 hours (weekends and holidays included) after the installation of the equipment has occurred or begins to occur; and 2) the authorization obtained applies only to that specific phone/facility - the use of a pen/trap on any additional phones or facilities that may be identified during the emergency situation need to authorized by the DAAG.

III. **Consent:** If the request pertains to the victim's phone or a phone used by someone who is cooperating with the investigation, consider whether consent would apply. The cooperating party may consent to the installation of a trap and trace/pen register on their phone, and with respect to the victim, consent may be implied depending on the circumstances. See 18 U.S.C. 3121(b)(2)("user" may consent)

PROCEDURES FOR EMERGENCY REQUESTS FOR CELL SITE DATA WHEN SOUGHT IN CONNECTION WITH A PEN/TRAP

I. **Justification:** See above

II. **Procedures:** See above. When advising the AUSA or agent about filing the application and proposed order, instruct them to file an application that cites to both the pen register/trap and trace statute and 18 U.S.C. 2703(d).

III. **Invocation of 18 U.S.C. 2702(c)(4) to receive prospective cell site:** Reliance on this provision to allow repeated, perspective collection of cell site data may be problematic. Judicious use of this provision is advised. Advise the field that the more prudent course of action is to obtain a search warrant under Rule 41 for repeated disclosures of prospective cell site information because Rule 41 has prospective effect.

IV. **Consent:** As with an emergency pen/trap request, consider whether consent would apply. See 18 U.S.C. 2702(c)(2) - allowing a provider to disclose a record or other information with the consent of the "customer or subscriber."

* **NOTE:** A service provider can voluntarily disclose **historical** cell site data under 18 U.S.C. 2702(c)(4), and follow-up compulsory process is unnecessary.

PROCEDURES FOR EMERGENCY REQUESTS FOR LATITUDE/LONGITUDE DATA FOR CELLULAR PHONES, I.E., GPS, E-911, TOWER TRILATERATION

The Department cannot authorize the collection of GPS (latitude/longitude) data, E-911 information, or location information generated through tower trilateration under the emergency pen/trap statute. (Tower trilateration measures the signal strength from multiple cell towers to locate the phone and is relatively accurate.) If law enforcement seeks this information, they need to obtain a search warrant under Rule 41, absent an emergency or voluntary disclosure by the service provider. Again, consent is an option if the target phone belongs to the victim or someone cooperating with the investigation.

When advising the field, ascertain if the service provider can actually produce the information.

* Sprint/Nextel: True GPS

* T-Mobile: Tower trilateration

* Verizon Wireless/Alltel: no GPS, unless the phone is used to call 911. Typically, these providers can only pinpoint the location of a cell phone within the "banana range" from a cell tower.

In addition, GPS data can only be captured when the phone is on and registering with the network. Providers do not maintain historical GPS/E-911 data. One exception is the "kiddie tracker" phone service.

One final consideration is where to obtain the warrant. Obtain the warrant where the phone is reasonably believed to be.

PROCEDURES FOR EMERGENCY WIRETAP REQUESTS
PURSUANT TO 18 U.S.C. 2518(7)

I. Justification:

A. A situation where there is: 1) an immediate threat to life or limb; 2) conspiratorial activity characteristic of organized crime; or 3) conspiratorial activity threatening national security; AND

B. An order cannot be obtained with an exercise of due diligence; AND

C. There are grounds upon which an order could be issued, i.e. probable cause for a predicate offense and/or federal felony (usually not an issue) and legal necessity.

II. Procedures:

A. Obtain the following, relevant facts: 1) circumstances giving rise to the emergency situation; 2) who, if known, is using the target phone/facility/location; 3) how the target phone/facility/location was identified; 4) when the phone/facility/location was last known to be used; 5) most recent criminal activity; and 6) basis for belief that phone/facility/location will be used for communications concerning the crime, i.e. what evidence is there that the perpetrator is acting in concert with others - what communications will be obtained.

B. Call a DAAG, through the Command Center, at (b)(6)&(7)(C) (b)(6)&(7)(C) and advise the official of the facts.

C. Once the DAAG concurs that an emergency situation exists, call the law enforcement officer or AUSA back and advise them of the following: 1) the Criminal Division agrees that an emergency tap may be sought; 2) the law enforcement officer must proceed up his chain of command to seek approval for the emergency tap; and 3) a high-level official of the law enforcement agency (for example, the Assistant Director or Director of the FBI) must contact either the AG, the DAG, or the AAG (Associate Attorney General) to obtain approval to proceed with the emergency tap.

D. Once the tap has been authorized by DOJ, the AUSA must file an application, affidavit, and proposed order within 48 hours after the interception has occurred or begins to occur. (Sample pleadings are available on USABook).

E. The affidavit in support of the emergency must contain only those facts known to the law enforcement officer at the time the emergency authorization was obtained from DOJ.

F. All pleadings must be reviewed by OEO before the AUSA goes to court.

G. Any documentation of the emergency authorization would come from the law enforcement agency and would include the date and time of the authorization, the identity of the authorizing official, and a description of the phone/facility/location that was authorized for interception, i.e., the phone number for the phone, the email address for the internet account, or the physical address of the location. This documentation should be filed with the AUSA's application. OEO/Criminal Division does not provide such documentation as we are not involved directly with the approval process at the AG/DAG/AAG level.

H. Continued surveillance: If the law enforcement agency wants to extend interceptions beyond the first 48-hour period, then:

1. They must seek DAAG authority to do so.

2. The affidavit filed in support of the emergency request may also include a section that provides probable cause to extend the interceptions. The affidavit must clearly differentiate between those facts in support of the emergency and those in support of the extension request.

3. Separate applications and orders should be filed for the emergency and extension requests.

USE OF WITT EQUIPMENT

WITT is a catchall term for equipment that law enforcement can use to locate a cellular phone. It includes devices called Wolfpack, Stingray, and Gossamer. WITT equipment emulates a cell phone tower and can be used to determine which direction the phone is in and how strong the signal is.

If law enforcement seeks to use their WITT equipment to locate a cellular phone, they need to obtain a pen register and trap and trace order for that phone. If they want to use the WITT equipment in an emergency situation, they must obtain DOJ approval first. Consent, for the reasons stated herein, may also apply.

The following form is designed for the purpose of identifying an unknown phone – that is, a phone whose identifying attributes are not known – being used/carried by a known individual.

In brief, the technique involves using field equipment owned and operated by the law enforcement agency to detect all powered-on phones in the immediate vicinity of the subject. (Carrier assistance is not normally required unless the subject's location is unknown.) The survey is repeated at various times and in various locations, ideally at least 3 or 4, in proximity to the subject. The end product is a list of wireless instruments present and operating at each location, where the element common to those lists – typically a single device – represents the identifier for the subject's phone.

Because the objective is simply to identify the unknown device, collection should be limited to device identifiers (e.g., IMEI, IMSI, MIN, etc.). It should not encompass dialed digits, as that would entail surveillance on the calling activity of all persons in the vicinity of the subject. Once the subject's phone is identified, you may obtain a conventional pen/trap order or other legal process addressed to the relevant carrier.

Finally, note that a separate form – not this form – should be employed for using law enforcement field equipment to determine the unknown physical location of a known phone.

Questions or comments about this form or the underlying technique may be directed to

(b)(6)&(7)(C)
Associate Director
Office of Enforcement Operations
(b)(6)&(7)(C)
(b)(6)&(7)(C)

Rev. 1.3 8-11-08

UNITED STATES DISTRICT COURT
FOR THE [ ] DISTRICT OF [ ]
[ ] DIVISION

IN THE MATTER OF THE	§	
APPLICATION OF THE UNITED	§	
STATES OF AMERICA FOR AN	§	Case No. _____
ORDER AUTHORIZING THE	§	
INSTALLATION AND USE	§	(UNDER SEAL)
OF A PEN REGISTER AND TRAP	§	
AND TRACE DEVICE	§	

ORDER

This matter comes before the Court pursuant to written and sworn application under 18 U.S.C. §§ 3122(a)(1) and 3127(5) by Assistant United States Attorney **[Name]** (Applicant), an Attorney for the Government as defined by Federal Rule of Criminal Procedure Rule 1(b)(1)(B), applying for an order authorizing the use of a pen register and trap & trace device to identify the telephone number or other unique information (such as the Electronic Serial Number (ESN), International Mobile Equipment Identity (IMEI), or Mobile Equipment Identifier (MEID)) identifying the telephone (hereinafter the "Subject Telephone") being used by [SUBJECT'S NAME] in connection with an ongoing criminal investigation.

Pursuant to 18 U.S.C. § 3123(a)(1), Applicant has certified that the information likely to be obtained by the proposed pen register and trap and trace device is relevant to an ongoing criminal investigation being conducted by [**Investigative Agency**] regarding **[Offense Description, such as: 18 U.S.C. §))]** by **[SUBJECT'S NAME IN CAPS]** (Subject). The identity of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied is unknown. The order applies to the wireless telephone believed to be operated by the Subject to transmit wire or electronic communications. The pen register or trap and trace device is to be applied in the vicinity of the Subject to determine the number or other identifier of the Subject Telephone.

THEREFORE, IT IS HEREBY ORDERED, pursuant to 18 U.S.C. § 3123, that agents of

[**Investigative Agency**] may install and use a pen register and trap and trace device anywhere in the United States to record or decode the telephone number or other unique information (such as the Electronic Serial Number (ESN), International Mobile Equipment Identity (IMEI), or Mobile Equipment Identifier (MEID)) necessary to identify the Subject Telephone. [**Investigative agency**] shall neither retain nor make affirmative investigative use of data acquired beyond that necessary to identify the Subject telephone more fully.

IT IS FURTHER ORDERED THAT this Order shall be effective for sixty (60) days from the date this Order is signed by the court. 18 U.S.C. §§ 3123(c).

IT IS FURTHER ORDERED THAT , pursuant to 18 U.S.C. § 3123(d), that the Application and this Order are herewith SEALED until otherwise ordered by this Court.

Signed on _____ 2008, at_____.

_____

United States Magistrate Judge
[_____] District of [_____]

UNITED STATES DISTRICT COURT
FOR THE _____ DISTRICT OF _____

IN THE MATTER OF THE	§	
APPLICATION OF THE UNITED	§	
STATES OF AMERICA FOR AN	§	Case No. _____
ORDER AUTHORIZING THE	§	
INSTALLATION AND USE	§	(UNDER SEAL)
OF A PEN REGISTER AND TRAP	§	
AND TRACE DEVICE	§	

APPLICATION

The United States of America, by and through the undersigned Assistant United States Attorney, applies for an order authorizing the use of a pen register and trap & trace device to identify wireless telephone devices being used by persons suspected of committing federal crimes. In support of this application, Applicant states the following:

1. Applicant is an "attorney for the Government" as defined by Fed. R. Crim. P. 1(b)(1)(B) and, therefore, may apply for an order authorizing the installation and use of a pen register and trap & trace device. 18 U.S.C. §§ 3122(a)(1), 3127(5).

2. Applicant certifies that [**Investigative Agency**] is conducting an ongoing criminal investigation regarding **[Offense Description]** by **[SUBJECT'S NAME]** (hereafter, "**Subject**"), who is using one or more unidentified wireless telephones; and that **Subject** is known to live at or frequent the following locations: [Address1,] [Address2, etc]. The identity of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied is unknown. The order applies to wireless telephone communications utilizing GSM, CDMA, iDEN, TDMA, UMTS, or analog protocols—which comprise the entirety of all cellular or PCS wireless telephone protocols currently used in the United States. The number or other identifier of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied is unknown and it is the purpose of the requested order to identify this unknown information, such as the electronic serial number (ESN), international mobile equipment identity (IMEI), international

mobile subscriber identity (IMSI), or mobile equipment identifier (MEID).[1] The information likely to be obtained from the pen register and trap & trace device is relevant to the aforementioned investigation because it will enable investigators to identify **Subject's** phone. 18 U.S.C. § 3122(b)(1) & (2).

3. Pursuant to 18 U.S.C. § 3123(a)(1), Applicant requests the Court issue an order authorizing the installation and use of a pen register and trap and trace device for a period of sixty (60) days to detect radio signals emitted from wireless cellular telephones in the vicinity of the Subject that identify the telephones (e.g., by transmitting the telephone's serial number and phone number) to the network for authentication. By determining the identifying registration data at various locations in which the Subject Telephone is reasonably believed to be operating, the telephone number corresponding to the Subject Telephone can be identified. Data transmitted during autonomous registration is not dialed or otherwise controlled by the telephone user. It is an autonomous transmission that occurs when the phone is turned on and periodically thereafter, regardless of whether a call is being made, and in fact, is clearly separate from the establishment or maintenance of a call.

4. Applicant further requests that this application any order entered in connection therewith be SEALED until otherwise ordered by the Court. Specifically, disclosure of the requested order and investigation would likely result in flight from prosecution, a modification of the **Subject's** activities or the activities of those with whom **Subject** communicates and associates, or the destruction or tampering of evidence; and would otherwise seriously jeopardize the investigation.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief, and that this declaration was executed on **[DATE]**, at _____.

_____

[1]Any potential interference to service occasioned by use of the Pen Register or Trap and Trace will be minimized so as to be no more disruptive than might ordinarily occur with cellular service coverage.

[APPLICANT]
Assistant U.S. Attorney_____
[TELEPHONE NUMBER]

The following form is designed for the purpose of identifying an unknown phone – that is, a phone whose identifying attributes are not known – being used/carried by a known individual.

In brief, the technique involves using field equipment owned and operated by the law enforcement agency to detect all powered-on phones in the immediate vicinity of the subject. (Carrier assistance is not normally required unless the subject's location is unknown.) The survey is repeated at various times and in various locations, ideally at least 3 or 4, in proximity to the subject. The end product is a list of wireless instruments present and operating at each location, where the element common to those lists – typically a single device – represents the identifier for the subject's phone.

Because the objective is simply to identify the unknown device, collection should be limited to device identifiers (e.g., IMEI, IMSI, MIN, etc.). It should not encompass dialed digits, as that would entail surveillance on the calling activity of all persons in the vicinity of the subject. Once the subject's phone is identified, you may obtain a conventional pen/trap order or other legal process addressed to the relevant carrier.

Finally, note that a separate form – not this form – should be employed for using law enforcement field equipment to determine the unknown physical location of a known phone.

Questions or comments about this form or the underlying technique may be directed to

(b)(6)&(7)(C)
Associate Director
Office of Enforcement Operations
(b)(6)&(7)(C)
(b)(6)&(7)(C)

Rev. 1.3 8-11-08

UNITED STATES DISTRICT COURT
FOR THE [ ] DISTRICT OF [ ]
[ ] DIVISION

IN THE MATTER OF THE	§	
APPLICATION OF THE UNITED	§	
STATES OF AMERICA FOR AN	§	Case No. _____
ORDER AUTHORIZING THE	§	
INSTALLATION AND USE	§	(UNDER SEAL)
OF A PEN REGISTER AND TRAP	§	
AND TRACE DEVICE	§	

ORDER

This matter comes before the Court pursuant to written and sworn application under 18 U.S.C. §§ 3122(a)(1) and 3127(5) by Assistant United States Attorney **[Name]** (Applicant), an Attorney for the Government as defined by Federal Rule of Criminal Procedure Rule 1(b)(1)(B), applying for an order authorizing the use of a pen register and trap & trace device to identify the telephone number or other unique information (such as the Electronic Serial Number (ESN), International Mobile Equipment Identity (IMEI), or Mobile Equipment Identifier (MEID)) identifying the telephone (hereinafter the "Subject Telephone") being used by [SUBJECT'S NAME] in connection with an ongoing criminal investigation.

Pursuant to 18 U.S.C. § 3123(a)(1), Applicant has certified that the information likely to be obtained by the proposed pen register and trap and trace device is relevant to an ongoing criminal investigation being conducted by [**Investigative Agency**] regarding **[Offense Description, such as: 18 U.S.C. §))]** by **[SUBJECT'S NAME IN CAPS]** (Subject). The identity of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied is unknown. The order applies to the wireless telephone believed to be operated by the Subject to transmit wire or electronic communications. The pen register or trap and trace device is to be applied in the vicinity of the Subject to determine the number or other identifier of the Subject Telephone.

THEREFORE, IT IS HEREBY ORDERED, pursuant to 18 U.S.C. § 3123, that agents of

[**Investigative Agency**] may install and use a pen register and trap and trace device anywhere in the United States to record or decode the telephone number or other unique information (such as the Electronic Serial Number (ESN), International Mobile Equipment Identity (IMEI), or Mobile Equipment Identifier (MEID)) necessary to identify the Subject Telephone. [**Investigative agency**] shall neither retain nor make affirmative investigative use of data acquired beyond that necessary to identify the Subject telephone more fully.

IT IS FURTHER ORDERED THAT this Order shall be effective for sixty (60) days from the date this Order is signed by the court. 18 U.S.C. §§ 3123(c).

IT IS FURTHER ORDERED THAT , pursuant to 18 U.S.C. § 3123(d), that the Application and this Order are herewith SEALED until otherwise ordered by this Court.

Signed on _____ 2008, at_____.

_____

United States Magistrate Judge
[_____] District of [_____]

UNITED STATES DISTRICT COURT
FOR THE _____ DISTRICT OF _____

IN THE MATTER OF THE	§	
APPLICATION OF THE UNITED	§	
STATES OF AMERICA FOR AN	§	Case No. _____
ORDER AUTHORIZING THE	§	
INSTALLATION AND USE	§	(UNDER SEAL)
OF A PEN REGISTER AND TRAP	§	
AND TRACE DEVICE	§	

APPLICATION

The United States of America, by and through the undersigned Assistant United States Attorney, applies for an order authorizing the use of a pen register and trap & trace device to identify wireless telephone devices being used by persons suspected of committing federal crimes. In support of this application, Applicant states the following:

1. Applicant is an "attorney for the Government" as defined by Fed. R. Crim. P. 1(b)(1)(B) and, therefore, may apply for an order authorizing the installation and use of a pen register and trap & trace device. 18 U.S.C. §§ 3122(a)(1), 3127(5).

2. Applicant certifies that [**Investigative Agency**] is conducting an ongoing criminal investigation regarding **[Offense Description]** by **[SUBJECT'S NAME]** (hereafter, "**Subject**"), who is using one or more unidentified wireless telephones; and that **Subject** is known to live at or frequent the following locations: [Address1,] [Address2, etc]. The identity of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied is unknown. The order applies to wireless telephone communications utilizing GSM, CDMA, iDEN, TDMA, UMTS, or analog protocols—which comprise the entirety of all cellular or PCS wireless telephone protocols currently used in the United States. The number or other identifier of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied is unknown and it is the purpose of the requested order to identify this unknown information, such as the electronic serial number (ESN), international mobile equipment identity (IMEI), international

mobile subscriber identity (IMSI), or mobile equipment identifier (MEID).[1] The information likely to be obtained from the pen register and trap & trace device is relevant to the aforementioned investigation because it will enable investigators to identify **Subject's** phone. 18 U.S.C. § 3122(b)(1) & (2).

3. Pursuant to 18 U.S.C. § 3123(a)(1), Applicant requests the Court issue an order authorizing the installation and use of a pen register and trap and trace device for a period of sixty (60) days to detect radio signals emitted from wireless cellular telephones in the vicinity of the Subject that identify the telephones (e.g., by transmitting the telephone's serial number and phone number) to the network for authentication. By determining the identifying registration data at various locations in which the Subject Telephone is reasonably believed to be operating, the telephone number corresponding to the Subject Telephone can be identified. Data transmitted during autonomous registration is not dialed or otherwise controlled by the telephone user. It is an autonomous transmission that occurs when the phone is turned on and periodically thereafter, regardless of whether a call is being made, and in fact, is clearly separate from the establishment or maintenance of a call.

4. Applicant further requests that this application any order entered in connection therewith be SEALED until otherwise ordered by the Court. Specifically, disclosure of the requested order and investigation would likely result in flight from prosecution, a modification of the **Subject's** activities or the activities of those with whom **Subject** communicates and associates, or the destruction or tampering of evidence; and would otherwise seriously jeopardize the investigation.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief, and that this declaration was executed on **[DATE]**, at _____.

_____

[1]Any potential interference to service occasioned by use of the Pen Register or Trap and Trace will be minimized so as to be no more disruptive than might ordinarily occur with cellular service coverage.

[APPLICANT]
Assistant U.S. Attorney_____
[TELEPHONE NUMBER]

Attachment A
TABLE OF TECHNICAL ELSUR TERMINOLOGY & AUTHORITIES (v20110912)

PEOPLE & ENTITIES: (alphabetical)

Attorney for the Government is defined by Fed. R. Crim. P. Rule 1(b)(1)(B) to include U.S. Attorneys and their assistants. Pursuant to 18 U.S.C. §§ 3122(applications) & 3127(5)(definitions), "[a]n Attorney for the Government may make application for an order [to a federal **court of competent jurisdiction**] authorizing or approving the installation and use of a **pen register** or a **trap and trace device[;]**" and a "**State investigative or law enforcement officer** may make [...such...] application...to a **court of competent jurisdiction of such State.**"

Court of Competent Jurisdiction is incorporated into chapter 206 of Title 18 (Pen Registers and Trap & Trace Devices) by 18 U.S.C. § 3127(2)(**PRTT** definitions) and into chapter 121 of Title 18 (Stored Communications & Transactional Records Access) by 18 U.S.C. § 2711(3)(**SCA** definitions), where it is defined to include any U.S. District Court (and their magistrate judges) that (i) has jurisdiction over the offense; *or* (ii) is in or for a district where a **communications provider** or other person/entity subject to the **PRTT assistance provisions** is located or where the communications, records or other information is stored; *or*, (iii) is acting pursuant to a **request for foreign assistance**. It includes "a court of general criminal jurisdiction of a State authorized by the law of that State to enter orders authorizing the use of a pen register or a trap and trace device[or issue search warrants.]" A federal court order authorizes installation and use "anywhere within the United States" whereas a state court order authorizes the same "within the jurisdiction of the court[.]" Because the interception has been federally-determined to occur both where law enforcement maintains its listening post and at the situs of the device, itself, state jurisdiction can be lawfully effected under chapter 206 on any provider within the U.S. irrespective of the provider's or the device's location whenever an interception occurs within the state. *U.S. v. Denman*, 100 F.3d 399, 402 (5th Cir. 1996) and *U.S. v. Tavarez*, 40 F.3d 1136 (10th Cir. 1994), *both citing, U.S. v. Rodriguez*, 968 F.2d 130 (2d Cir.), *cert den'd.*, 113 S.Ct. 139, 140 & 663 (1992). States are, therefore, confined only by their own long-arm statutes or common law interpretation of *where* an intercept might otherwise occur.

"[A] **Fugitive from Justice** has been defined as '[a] person who, having committed a crime, flees from [the] jurisdiction of [the] court where [a] crime was committed or departs from his usual place of abode and conceals himself within the district.'" *Empire Blue Cross & Blue Shield v. Finkelstein*, 111 F.3d 278, 281 (2d Cir. 1997)(quoting Black's Law Dictionary 604 (5th ed. 1979)). *See, e.g.*, 18 U.S.C. § 1071. A fugitive from justice enjoys no protected privacy interest in his physical location. *See, e.g., U.S. v. Jacobsen*, 466 U.S. 109, 113 (1984)(a "search" occurs "when an expectation of privacy that society is prepared to consider reasonable is infringed.") Like contraband, a fugitive is subject to seizure anytime, anywhere; and may be tracked and arrested into otherwise private areas, even absent search warrant, with no basis to complain. *Steagald v. U.S.*, 451 U.S. 204, 222 (1981)(Although search warrants are available to aid in locating and capturing a fugitive inside a non-public location that would otherwise enjoy a reasonable expectation of privacy, no search warrant is necessary to invade the sanctity of a fugitive's residence. In contrast, a search warrant to locate a fugitive is available to, and required of, law enforcement when, absent exigent circumstances, they seek to invade the sanctity of some third party's residence. In either case, a fugitive for whom an arrest warrant has issued has no standing to object to the otherwise warrantless invasion of privacy and arrest in either his own residence or that of another person.). *See, also, U.S. v Pringle,* 576 F.2d 1114 (5th Cir. 1978)(use of beeper in tracking package constitutionally permissible, observing that possessors of contraband have no legitimate expectation of privacy in substances which they have no right to possess at all).

Investigative or Law Enforcement Officer is undefined by chapter 206 (Pen Registers and Trap and Trace Devices) of Title 18 but is defined in chapter 119 (colloquially, "wiretap") of Title 18 at § 2510(7)(definitions) as "any officer of the United States or of a State or political subdivision thereof, who is empowered by law to conduct investigations of or to make arrests for offense enumerated in [chapter 119, constituting serious felony offenses], and any attorney authorized by law to prosecute or participate in the prosecution of such offenses."

State is defined by 18 U.S.C. § 3127(6) to include all states, territories or possessions of the United States.

Task Force Operating under Special Apprehension Authority means a U.S. Marshals Service (USMS) fugitive task force operating pursuant to the Attorney General's 1994 directive to subordinate Department of Justice (DOJ) agencies and offices to establish and coordinate federal, state and local law enforcement task forces to combat violent crime. *See* Attorney General's March 1, 1994 Memorandum to All United States Attorneys, Implementation of National Anti-Violent Crime Initiative (NAVCI). In 1988, Congress granted the Attorney General authority to direct agents of the USMS to "investigate such fugitive matters, both within and outside the United States[.]" 28 U.S.C. § 566(e)(1)(B). Formal recognition of USMS authority to pursue non-federal fugitives in the absence of a federal crime (such as "UFAP" at 18 U.S.C. § 1073) is based on a long history of federal fugitive assistance to local and state authorities – both within and beyond the several states' jurisdictional reach. *See* Department of Justice Office of Legal Counsel's February 21, 1995 opinion, Authority to Pursue Non-Federal Fugitives and Department of Justice Policy on Fugitive Apprehension (Aug. 11, 1988). Congress later authorized and appropriated funding for the Presidential Threat Protection Act of 2000 (Pub. L. 106-544)("PTPA"), which mandated creation of USMS-led federal, state and local task forces for the specific purpose of pursuing and apprehending state fugitives. At the close of CY 2010, seventy five (75) NAVCI District Fugitive Task Forces, seven (7) PTPA Regional Fugitive Task Forces and a multitude of national or regionally-coordinated Fugitive Investigative Strike Team ("FIST") operations (such as FALCON) operated pursuant these Congressional mandates and Attorney General authorizations. This history, legislation and funding demonstrates the Congress' clear intent to make the full array of federal authority, expertise and investigative tools – *including* access to federal judicial process – available to the Service when performing its federal duties in pursuing state fugitives. *See, e.g.,* September 14, 2004 Department of Justice Report to Congress, Fugitive Apprehension. The assertion that federal legal process is available for the USMS' federal investigations of state fugitives is supported by the fact that, like chapters 121 (Stored Communications) and 206 (Pen Register and Trap & Trace), Federal Rule of Criminal Procedure 41(c)(4)(search warrant for "a person to be arrested") does not require a predicate federal offense. *Cf. c*hapter 119 (Wiretap) at 18 U.S.C. § 2516(1)(defining a limited set of federal offenses for which a federal wire communications intercept order may issue) and (3)(defining any "Federal felony" as a prerequisite to s federal electronic communications intercept order).

INTERCEPT/INFORMATION/RECORDS/TRANSACTIONAL DATA TERMS:
(grouped as pertinent to a Hybrid PRTT introduction and discussion)

Wire Communication is defined by 18 U.S.C. § 2510(1) and is incorporated into **PRTT** law by 18 U.S.C. § 3127(1) to mean an "aural transfer [(human voice)] made in whole or in part…by, cable or other like connection…furnished or operated by any" **Communications Provider** engaged in or "affecting in interstate or foreign commerce." In essence, it is the spoken word carried from one person to another, remotely-located, person but does not include radio communications.

Electronic Communication is defined by 18 U.S.C. § 2510(12) and is incorporated into **PRTT** law by 18 U.S.C. § 3127(1) to mean "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce[.]" In essence, it is text messages, email, instant messaging, pictures, videos, documents, attachments, or any other data that is carried across the internet or transmitted by radio frequency (including cellular/wireless infrastructure). It does not include wire (aural transfer) or oral (spoken word) communications, electronic funds transfer information, or any communication through a tone-only pager or made from a tracking device.

Electronic Communications Service is defined by 18 U.S.C. § 2510(15) and is incorporated into **PRTT** law by 18 U.S.C. § 3127(1). Confusing by its inclusion of the shorter phrase "electronic communication" (which *excludes* wire communications), an **electronic communications service** *includes* "any service which provides to users thereof the ability to send or receive wire or electronic communications."

Contents is defined by 18 U.S.C. § 2510(8) and is incorporated into **PRTT** law by 18 U.S.C. § 3127(1) to mean "any information concerning the substance, purport, or meaning of that communication." It does not include the non-content "transactional records" contemplated for disclosure, retrospectively, under **SCA** or**,** prospectively, under **PRTT**.

Trap and trace device (or **TT**) is defined by 18 U.S.C. § 3127(4) as "a device or process that captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication[.]"

Pen register (or **PR**) is defined by 18 U.S.C. § 3127(3) as a "device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication[.]"

Scanning Receiver is defined at 18 U.S.C. § 1029(e)(8) as "a device or apparatus that can be used to intercept is to intercept an electronic serial number, mobile identification number, or other identifier of any telecommunications service, equipment, or instrument." Improper use is punishable under subsection (a)(8) of this same section by up to 15 years confinement for a first offense. Law enforcement is exempted.

Telecommunication Identifying Information is defined at 18 U.S.C. § 1029(e)(11) as an "electronic serial number or any other number or signal that identifies a specific telecommunications instrument or account, or a specific communication transmitted from a telecommunications instrument." Improper use or possession of "hardware or software, knowing it has been configured to insert or modify telecommunication identifying information associated with or contained in a telecommunications instrument so that such instrument may be used to obtain telecommunications service without authorization," is punishable under subsection (a)(9) of this same section by up to 15 years confinement for a first offense. Law enforcement is exempted.

"**Post cut-through dialed digits**," also called "dialed digit extraction features," are any digits dialed from a target device after the initial call setup is completed; and are necessary to identify, *inter alia*, the true destination of a call made with a calling card. The government can ordinarily capture these through use of a **PR**. By DOJ policy, pursuant to the limitations of 18 U.S.C. § 3121(c) and consistent with the definitions in 18 U.S.C. § 3127, an investigative agency shall use technology reasonably available to it that (a) restricts the recording or decoding of electronic or other impulses to the dialing, routing, addressing, and signaling information utilized in the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications; (b) implements the pen register and trap and trace unobtrusively while minimizing interference, if any, with the services that the telecommunications provider accords all of its customers; and, (c) shall neither retain nor make affirmative investigative use of any over-collected or non-targeted data. Unless specifically requested in the Application but without conceding the issue, the government does not request an order expressly authorizing access to post cut-through dialed digits, which may occasionally include communicative content which the government – absent human receipt and review – is unable to conclusively distinguish from non-content. *In the Matter of the Application of the U.S.*, 622 F.Supp.2d (S.D.Tex. 2007)(USDJ slip op, supporting, in part, the USMJ holdings in 441 F.Supp.2d 816, 818); *In the Matter of the Application of the United States of America,* No. 06-MJ-1130 (M.D. Fla. June 20, 2006)(unreported); *but see, In re U.S. for an Order*, 632 F.Supp.2d 202 (E.D.N.Y 2008)(reversing and remanding with instructions to the USMJ to issue an order to include PCTDD, based upon government's affirmative statement that it would delete PCTDD upon receipt) and 2008 WL 5255815 (same USMJ who was reversed refusing to follow the USDJ's remand instruction and yet-denying the application, as he had previously for similar applications in 515 F.Supp.2d 325).

PRTT is an acronym meaning both a pen register and trap and trace device and PRTT law as defined in chapter 206 of Title 18 at §§ 3121-3127. PRTT orders "shall" issue when the **Attorney for the Government** (or **State investigative or law enforcement officer**, in **State** court) "has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation." In this respect, the court's role is ministerial because the government is not required to offer evidence or to present any factual basis. Under § 3123(a)(1), federal PRTT orders are effective "anywhere within the United States." Under § 3123(a)(2), **State** PRTT orders are effective "within the jurisdiction of the court" – thus leaving geographic/long-arm jurisdictional matters up to the States' own legislative or judicially-imposed constraints.

PRTT capabilities and assistance provisions means the capabilities standards and assistance required of **Communications Providers** or other persons/entities under the Communications Assistance for Law Enforcement Act of 1994 ("**CALEA**")(codified in part at 18 U.S.C. § 3124). This requires "all information, facilities, and technical assistance necessary to accomplish the installation of the pen register unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place." **Communications Providers** will frequently decline to offer certain types of assistance (such as "account takeover" continuation of services or assigning a static IP address to a targeted account or sending records via email) unless expressly required as a component to an order's assistance provisions.

Communications Provider is used to mean not only the "telecommunications carriers" initially contemplated under early **PRTT** law and **CALEA**, but also includes any wire or electronic communications service provider. In this sense, it covers almost any conceivable provider of communications services, including applications providers.

Cell-Site Location Information, *or* **CSLI**, means records or other information concerning the antenna (or discrete tower/sector) of a communications provider's infrastructure through which a subscriber's wire or electronic communication is carried, typically limited to the beginning or end of a call, text message or data session, by virtue of the "punch list" specifications to **CALEA**'s J-Std25A capabilities standards. *See U.S. Telecom Ass'n v. F.C.C.*, No. 99-1442, 227 F.3d 450 (D.C. Cir. Aug. 15, 2000), *affirming* FCC Third Report & Order (FCC 99-230, Docket No. 97-213 (Aug. 31, 1999)). When used to refer to prospective CSLI captured as part of a **PRTT** installation across a CALEA-compliant connection, this class of information may also be referred to as "cell site location routing information" because it identifies the "dialing, routing, addressing or signaling" component of a **PR** or **TT**.

CALEA location caveat means the **communications provider** disclosure restriction in **CALEA**, codified at 47 U.S.C. § 1002(a)(2)(B), which states: "with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices…such call-identifying information shall not include any information that may disclose the physical location of the subscriber[.]" Despite this disclosure restriction (creating an authorities question), cell sites remain within the definition, at 18 U.S.C. 3127, of what a pen register and trap and trace device are (as routing information). This is the crux of the **Hybrid Theory** vs. R.41 debate with respect to **CSLI**.

SCA means the "Stored Wire and Electronic Communications and Transactional Records Access" statutes found in chapter 121 of Title 18 at §§ 2701 – 2712, which were promulgated by Title II of the 1986 Electronic Communications Privacy Act (ECPA). The SCA sets three evidentiary tiers for government access to communications provider records/information: (i) subpoenas may issue without factual basis or court oversight for a narrowly defined set of ordinary business records found in § 2703(c)(2)(A)-((F); (ii) court orders may issue under § 2703(d) for a "record or other information" (defined in § 2703(c) to exclude content unless it is old (defined under 2703(a) as older than 180 days) or remotely-stored (as specified in § 2703(b)) when the government offers "specific and articulable facts showing that there are reasonable grounds to believe that the contents…or the records or other information sought, are relevant and material to an ongoing criminal investigation;" and, (iii) warrants issue under authority of § 2703(c)(1)(A) "using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant." This has been universally accepted to mean the procedures of Fed. R. of Crim. P. 41 (and its probable cause requirement).

Transactional records means all non-content **PRTT** or stored "records or other information" associated with a communication, such as the origin/destination/parties (dialing/addressing/conferencing) or routing/signaling (e.g. switching or IP path or radio frequency/handshake/automated messaging information) associated with wire or electronic communications. Government access to historical transactional records is governed by **SCA** while access to prospective, real-time transactional records (including CSLI) is governed by **PRTT** law, as further described below.

Subpoena-class subscriber records defines a class of non-content subscriber records for which there is no constitutionally-recognizable reasonable expectation of privacy and which Congress has made available to the government, pursuant to 18 U.S.C. § 2703(c)(2)(A)-(F), upon issuance of a federal or state administrative, grand

jury or trial subpoena. These records are the least protected communications subscriber records under the law and include: "(A) name; (B) address; (C) local and long distance telephone connection records, or records of session times and durations [under 47 CFR § 42.6, for up to the preceding eighteen (18) months]; (D) length of service (including start date) and types of service utilized; (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; (F) means and source of payment for such service (including any credit card or bank account number)[.]"

Derivative-class subscriber records means, with respect to unique target identities determined by virtue of the court order to be originating communications to, or receiving communications from, the listed unique target identity (i.e. people communicating with the target), all of the foregoing **subpoena-class subscriber records** except "means and source of payment" but including, pursuant to 18 U.S.C. § 2703(c) & (d)(requiring a court order based on submission of "specific and articulable facts" establishing materiality and relevance), date of birth, social security number, driver's license number, alternate contact numbers, addresses and employment information. These records are useful to law enforcement in identifying persons and locations for interview, investigation or surveillance; in confirming/completing the addressing and routing of communications originating from or terminating to the targeted identity; and in identifying prior, additional or subsequent communications identities utilized by the suspect under investigation. A request for this type of discrete and clearly-defined class of records is supported by the holding in *U.S. v. Fregoso*, 60 F.3d 1314, 1321 (8th Cir. 1995)(because the logical ends to a pen register or trap and trace device installation is to further an investigation by identifying the suspect's communicants; and, when disclosed with the trap and trace device, "acquisition and use of the subscriber information ['revealed to the phone company' carried 'no legitimate expectation of privacy' and] did not violate federal law"). When the government establishes that the entire class is relevant and material to the ongoing criminal investigation, such an authorization promotes judicial economy by eliminating the need to return to the court on a daily basis with a lengthy list of derivative "2703(d)-applications" seeking an order for disclosure of otherwise unprotected information. Importantly, the USMS lacks administrative subpoena authority and does not have access to grand jury or trial subpoenas. *In re Pedro Archuleta*, 432 F. Supp. 583 (S.D.N.Y. 1977); *In re Wood*, 430 F. Supp. 41 (S.D.N.Y. 1977), *aff'd sub nom In re Cueto*, 554 F.2d 14 (2d Cir. 1977).

Target-class subscriber records means, with respect to the listed unique target identifier, the foregoing **derivative-class subscriber records** with "means and source of payment" and the additional requirement to identify additional telephone or instrument numbers/identities on the same account as the targeted identity and any alternate contact numbers, employment information or other information collected with account registration or maintenance. These additional records are useful to law enforcement in identifying the suspect's financial information and activities, additional or subsequent communications identities utilized by the suspect under investigation, and information which may have been provided prior to an attempt to conceal information for, or as a result of, criminal activity.

Hybrid Theory means the court-approved use of a prospectively-effective **PRTT** authorization coupled with an accompanying/contemporaneous order under **SCA** (establishing what amounts to "reasonable suspicion") for the "disclos[ure of] a record or other information pertaining to s subscriber to or customer of [a communications provider] (not including the contents of communications) when the governmental entity—obtains a court order for such disclosure under [18 U.S.C. § 2703(d)]." The premise behind the Hybrid Theory is that the **CALEA location caveat**, which prohibits disclosure of cell site location information "*solely pursuant to*" **PRTT** authority, does not specify what the appropriate statutory/procedural mechanism and evidentiary standard to obtain **CSLI** actually is. Because **CSLI** identifies the first or last physical path through which wire or electronic communications are carried through a **Provider's** infrastructure to a subscriber, customer or user, **CSLI** clearly falls within the post-2001 USA PATRIOT ACT's modifying addition to the definitions of a "pen register" and of a "trap and trace device" (to include "addressing, routing, and signaling information") when received at real (or "near-real") time by law enforcement. Thus, Hybird Theory advocates assert that **CSLI** remains an incontrovertible component of **PRTT** – but that **CSLI** is simply not available without a **PRTT** order *plus something more*. Following the holdings of *United States v. Miller*, 425 U.S. 435 (1976) and *Smith v. Maryland*, 442 U.S. 735 (1979), Hybrid Theory advocates assert that there is no constitutional privacy interest in **CSLI** because this data is automatically, necessarily, voluntarily and, arguably, knowingly, disclosed to the third-party communications provider as a necessary and incident aspect of obtaining and using the wireless communications services to which the subscriber subscribes.

Some Hybrid Theory-endorsing courts make clear that the **communications provider** must receive/record (if even for a split-second) the **CSLI** before transmitting it to the government – while others simply permit the **SCA** to fill the **CALEA location caveat** void without exerting a great deal of focus on the **SCA's** apparently (although nowhere expressly stated) retrospective nature. Finally, Hybrid Theory advocates assert that the Congress is – and has been for more than a decade – acutely aware that law enforcement has been relying on this theory for as many years; and that when Congress considered but failed to pass legislation that would have elevated the evidentiary standard for obtaining prospective **CSLI** to probable cause, it implicitly approved of the continuing Hybrid Theory practice. 106 H. Rep. 932 (106th Cong, 2d Sess, Oct 4, 2000) on 106 H.R. 5018 ("[T]he government should have the ability to locate suspected criminals…[but there are] no clear legal standards governing when the government can collect location information from cell phone companies. Law enforcement now uses its authority under 18 U.S.C. Section(s) 2703(d)…to obtain location information from mobile phone service providers.") Credible challenges to the Hybrid Theory are discussed in the **Default Warrant Theory**, below.

Default Warrant Theory means an approach accepted by courts which reject the **Hybrid Theory**, either because of a lack of express Congressional intent or because they do not believe that the **SCA** has any prospective efficacy (even when combined with a prospectively-effective **PRTT** order). Default Warrant Theory advocates assert that unless Congress has expressly articulated otherwise through legislation, obtaining a search warrant under Fed. R. of Crim. P. 41 is the only way to gain government access to property/information – even information not enjoying a constitutionally-recognized reasonable expectation of privacy – when the person or entity whose property/information at issue is unwilling or unable to disclose it to the government, whether voluntarily or pursuant to subpoena. As applied to **CSLI**, advocates of this approach believe that while **CSLI** enjoys no constitutionally-recognized reasonable expectation of privacy and remains the property of the **communications provider** and not the subscriber, the government is obliged to pursue a search warrant because (i) a **communications provider** is prohibited under **PRTT** from voluntarily disclosing prospective **CSLI** in the absence of a court or properly-declared emergency; and, (ii) Congress failed to specify any lesser statutory mechanism by which to overcome the **CALEA location caveat.** Proponents of the Default Warrant Theory accept the assertion that nationwide efficacy of a federal district search warrant is appropriate under Rule 41(a)(1)(special circumstances jurisdiction) because both 18 U.S.C. §§ 2703(c)(1)(A)(search warrants under SCA for "records or other information") and 3123 (PRTT orders) confer nationwide jurisdiction. That is, jurisdiction exists under chapter 206 of Title 18, despite that procedure and the government's burden of proof are defined by Fed. R. Crim. P. 41.

Tracking Device Theory means an approach accepted by courts which reject both the **Hybrid Theory** and the **Default Warrant Theory** because they conclude at the outset that since **CSLI** is created by an electronic device (i.e. cell phone) and loosely "permits the tracking of the movement of a person or object," that a strict and literal reading of 18 U.S.C. § 3117 requires treatment of **CSLI** as a tracking device. The small handful of advocates of this approach then point to 18 U.S.C. § 2510(12)(c) to conclude that **CSLI**, as a tracking device, becomes expressly *excluded* from the definition of an **electronic communication**…meaning **CSLI** enjoys no civil/criminal liability protection or treatment under **PRTT** law. Tracking Device Theory advocates believe, therefore, that **CSLI** does not enjoy a constitutionally-reasonable expectation of privacy unless otherwise-provided under applicable tracking device common law (generally limited to places not visible to the public; *c.f.* **Collage REP Theory**, below). Thus, under the **Tracking Device Theory**, the only reason the government would need an order or warrant would be to *compel* **Provider** disclosure of **CSLI** if/when a **Provider** is unwilling to provide such records voluntarily, as there would otherwise be no prohibition against a **Provider's voluntarily** disclosing **CSLI** to the government or any other third party. Problems with the Tracking Device Theory include the facts that:

(i) any business record (e.g. credit card transactions, ATM machines, toll passes, etc.) which creates a date/time/location stamp instantly becomes something it was not intended to be: a "tracking device" (violating the "primarily useful doctrine" described in *United States v. Herring*, 993 F.2d 784 (11th Cir. 1993)(in prohibiting unauthorized manufacture, assembly, possession or sale of *intercepting* devices under 18 U.S.C. §2512(1)(b), Congress included a requirement that "the design of the device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications"), *cert den'd,* 510 U.S. 933 (1993);

(ii) under 18 U.S.C. 2510(12)(c), only **CSLI** associated with communications *from* (the **PR** side) the phone become tracking device records, while all communications *to* (the **TT** side) the phone remain electronic communications;

(iii) no "installation" of a "device" can occur, since the **CSLI** is generated not by the phone (a device) but by an electronic communications *process* (call routing) that predates any court authorization (in fact, the only "device" for which a location is captured, stored and recorded correlates not to the phone handset, but is, instead, to the phone company's own cell tower);

(iv) because no "installation" of a "device" can occur, a federal district court lacks jurisdiction, under 18 U.S.C. 3117(a), to authorize use of the device "outside that jurisdiction if the device is installed in that jurisdiction[;]"

(v) there are no statutory criminal/civil penalties associated with a wrongful tracking device installation (and no reimbursement provision for a lawful installation) as there are under 18 U.S.C. 3121 for either a wrongful or proper **PRTT** installation.

Collage REP Theory means the approach articulated under *U.S. v. Maynard*, 615 F.3d 544, 392 U.S. App. D.C. 291 (D.C. Cir. 2010), cert. granted, *United States v. Jones*, 2011 WL 1456728 (June 27, 2011), wherein the government's collection of tracking device records, none of which individually violate a person's reasonable expectation of privacy, over a substantial and extended period of time (when the government might not reasonably have been lawfully present the entire time – such as the 28 days considered in the *Maynard* decision) collectively violate a reasonable expectation of privacy because they paint a "collage" of the person's activities not otherwise reasonably obtainable by the government despite that each record was taken in a public location and might otherwise stand alone. This approach is adhered to by a small handful of **Tracking Device Theory** advocates but has been expressly rejected by the 3rd Circuit as inapplicable to historical **CSLI**. In re Application of U.S. for an Order, F.3d 304, 313 (3rd Cir. 2010)(rejecting also, in dicta at 312, any application to prospective **CSLI**).

Device identity or hardware changes means the utility to the criminal element of public identity changes (e.g. mobile directory number, or MDN, being the 10-digit telephone number that we share with others, or an email address, etc.), hardware changes (e.g. electronic serial number, mobile equipment identifier or international mobile equipment identity, a/k/a ESN/MEID/IMEI) and, particularly, "SIM-swapping" and other network identity changes (e.g. subscriber identity module/international mobile subscriber identity (SIM/IMSI) and mobile subscriber identity/mobile identification number (MSID/MIN) changes) – in addition to the prolific use of prepay and anonymous/disposable accounts and phones – as an expeditious and inexpensive means of eluding and delaying law enforcement efforts to timely implement and maintain lawful intercepts. In recognition of rapidly emerging and changing technologies, the 2001 USA PATRIOT Act amended 18 U.S.C. § 3123(b)(1)(C) to require the Court to specify in the order "the attributes of the communications to which the order applies, including the number or other identifier[.]" This language mirrors the pre-existing requirement in wiretap law, at 18 U.S.C. § 2518(1)(b), for "a full and complete statement of the facts and circumstances relied upon by the applicant, to justify his belief that an order should be issued, including ... a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted." When new hardware or network identities are *matched* (by the provider) or *mated* (by the user) to prior hardware or identities and remain directly traceable to hardware or identities specified in the Order, the Court may authorize the continued intercept of transactions or communications across these changes. *See United States v. Duran*, 189 F.3d 1071, 1083-86 (9th Cir. 1999), *cert. den'd,* 529 U.S. 1081 (2000) (holding interception of wire communications on a cellular telephone with a changed telephone number followed by a changed ESN was subsumed within an order authorizing the interception of wire communications – even though the court order authorizing the wiretap only anticipated a changed telephone number but did not anticipate a changed ESN). In this respect, the Ninth Circuit affirmed the trial court's assessment that "[t]he original number to any changed number, to any instrument, is capable of being traced back to the original number, and therefore, the chain remains intact.... The order is broad enough to cover changes in the telephone number, and changes in the instrument.") A decade later this holding remains unchallenged; and the courts' authority and

practice of authorizing law enforcement intercepts to continue across hardware and/or identity mutations has become an investigative cornerstone to combating an increasingly tech-savvy criminal adversary.

Data-Specific Provisions apply to an Internet service provider (ISP, such as AT&T's uVerse service, Comcast's Xfinity service, etc.), Voice over Internet Protocol provider (VoIP, a type of telephony such as provided by Vonage and other "digital phone" providers, particularly ISPs), email (e.g. Yahoo or Gmail), Peer-to-Peer provider (e.g. Skype, a type of VoIP that does not typically interconnect to the public-switched telephone network, or PSTN) or social networking provider (e.g. Facebook, MySpace, Twitter or similar services where people share information about themselves through online "portals"). Users of these services must typically "authenticate" their right to use the service by username/password or alternate identity (e.g. mobile access control, or MAC, address, which is an ESN-like unique identifier assigned to a network appliance). These providers record access and communications through the data-equivalent to "toll" or "call detail records" (CDR includes "toll," or per-communication charged activity, as well as other transactional records) that are called connection and IP logs. A component to a complete connection or IP log is the port number through which a communication is carried. For example, all standard internet traffic passes across port 80 while standard-encryption internet traffic transits port 443; and wireless providers may assign a multitude of mobile customers the same IP address, differentiating their network traffic by port number. Knowing the port number does not disclose the contents of the communication. The destination port may characterize the types of services utilized while the source port can assist law enforcement in identifying and resolving to a specific subscriber account an IP address identified pursuant to an intercept order.

The following form is designed for the purpose of identifying an unknown phone – that is, a phone whose identifying attributes are not known – being used/carried by a known individual.

In brief, the technique involves using field equipment owned and operated by the law enforcement agency to detect all powered-on phones in the immediate vicinity of the subject. (Carrier assistance is not normally required unless the subject's location is unknown.) The survey is repeated at various times and in various locations, ideally at least 3 or 4, in proximity to the subject. The end product is a list of wireless instruments present and operating at each location, where the element common to those lists – typically a single device – represents the identifier for the subject's phone.

Because the objective is simply to identify the unknown device, collection should be limited to device identifiers (e.g., IMEI, IMSI, MIN, etc.). It should not encompass dialed digits, as that would entail surveillance on the calling activity of all persons in the vicinity of the subject. Once the subject's phone is identified, you may obtain a conventional pen/trap order or other legal process addressed to the relevant carrier.

Finally, note that a separate form – not this form – should be employed for using law enforcement field equipment to determine the unknown physical location of a known phone.

Questions or comments about this form or the underlying technique may be directed to

(b)(6)&(7)(C)
Associate Director
Office of Enforcement Operations
(b)(6)&(7)(C)
(b)(6)&(7)(C)

Rev. 1.3 8-11-08

UNITED STATES DISTRICT COURT
FOR THE [ ] DISTRICT OF [ ]
[ ] DIVISION

IN THE MATTER OF THE	§	
APPLICATION OF THE UNITED	§	
STATES OF AMERICA FOR AN	§	Case No. _____
ORDER AUTHORIZING THE	§	
INSTALLATION AND USE	§	(UNDER SEAL)
OF A PEN REGISTER AND TRAP	§	
AND TRACE DEVICE	§	

ORDER

This matter comes before the Court pursuant to written and sworn application under 18 U.S.C. §§ 3122(a)(1) and 3127(5) by Assistant United States Attorney **[Name]** (Applicant), an Attorney for the Government as defined by Federal Rule of Criminal Procedure Rule 1(b)(1)(B), applying for an order authorizing the use of a pen register and trap & trace device to identify the telephone number or other unique information (such as the Electronic Serial Number (ESN), International Mobile Equipment Identity (IMEI), or Mobile Equipment Identifier (MEID)) identifying the telephone (hereinafter the "Subject Telephone") being used by [SUBJECT'S NAME] in connection with an ongoing criminal investigation.

Pursuant to 18 U.S.C. § 3123(a)(1), Applicant has certified that the information likely to be obtained by the proposed pen register and trap and trace device is relevant to an ongoing criminal investigation being conducted by [**Investigative Agency**] regarding **[Offense Description, such as: 18 U.S.C. §))]** by **[SUBJECT'S NAME IN CAPS]** (Subject). The identity of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied is unknown. The order applies to the wireless telephone believed to be operated by the Subject to transmit wire or electronic communications. The pen register or trap and trace device is to be applied in the vicinity of the Subject to determine the number or other identifier of the Subject Telephone.

THEREFORE, IT IS HEREBY ORDERED, pursuant to 18 U.S.C. § 3123, that agents of

[**Investigative Agency**] may install and use a pen register and trap and trace device anywhere in the United States to record or decode the telephone number or other unique information (such as the Electronic Serial Number (ESN), International Mobile Equipment Identity (IMEI), or Mobile Equipment Identifier (MEID)) necessary to identify the Subject Telephone. [**Investigative agency**] shall neither retain nor make affirmative investigative use of data acquired beyond that necessary to identify the Subject telephone more fully.

IT IS FURTHER ORDERED THAT this Order shall be effective for sixty (60) days from the date this Order is signed by the court. 18 U.S.C. §§ 3123(c).

IT IS FURTHER ORDERED THAT , pursuant to 18 U.S.C. § 3123(d), that the Application and this Order are herewith SEALED until otherwise ordered by this Court.

Signed on _____ 2008, at_____.

_____

United States Magistrate Judge
[_____] District of [_____]

UNITED STATES DISTRICT COURT
FOR THE _____ DISTRICT OF _____

IN THE MATTER OF THE	§	
APPLICATION OF THE UNITED	§	
STATES OF AMERICA FOR AN	§	Case No. _____
ORDER AUTHORIZING THE	§	
INSTALLATION AND USE	§	(UNDER SEAL)
OF A PEN REGISTER AND TRAP	§	
AND TRACE DEVICE	§	

APPLICATION

The United States of America, by and through the undersigned Assistant United States Attorney, applies for an order authorizing the use of a pen register and trap & trace device to identify wireless telephone devices being used by persons suspected of committing federal crimes. In support of this application, Applicant states the following:

1. Applicant is an "attorney for the Government" as defined by Fed. R. Crim. P. 1(b)(1)(B) and, therefore, may apply for an order authorizing the installation and use of a pen register and trap & trace device. 18 U.S.C. §§ 3122(a)(1), 3127(5).

2. Applicant certifies that [**Investigative Agency**] is conducting an ongoing criminal investigation regarding **[Offense Description]** by **[SUBJECT'S NAME]** (hereafter, "**Subject**"), who is using one or more unidentified wireless telephones; and that **Subject** is known to live at or frequent the following locations: [Address1,] [Address2, etc]. The identity of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied is unknown. The order applies to wireless telephone communications utilizing GSM, CDMA, iDEN, TDMA, UMTS, or analog protocols—which comprise the entirety of all cellular or PCS wireless telephone protocols currently used in the United States. The number or other identifier of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied is unknown and it is the purpose of the requested order to identify this unknown information, such as the electronic serial number (ESN), international mobile equipment identity (IMEI), international

mobile subscriber identity (IMSI), or mobile equipment identifier (MEID).[1] The information likely to be obtained from the pen register and trap & trace device is relevant to the aforementioned investigation because it will enable investigators to identify **Subject's** phone. 18 U.S.C. § 3122(b)(1) & (2).

3. Pursuant to 18 U.S.C. § 3123(a)(1), Applicant requests the Court issue an order authorizing the installation and use of a pen register and trap and trace device for a period of sixty (60) days to detect radio signals emitted from wireless cellular telephones in the vicinity of the Subject that identify the telephones (e.g., by transmitting the telephone's serial number and phone number) to the network for authentication. By determining the identifying registration data at various locations in which the Subject Telephone is reasonably believed to be operating, the telephone number corresponding to the Subject Telephone can be identified. Data transmitted during autonomous registration is not dialed or otherwise controlled by the telephone user. It is an autonomous transmission that occurs when the phone is turned on and periodically thereafter, regardless of whether a call is being made, and in fact, is clearly separate from the establishment or maintenance of a call.

4. Applicant further requests that this application any order entered in connection therewith be SEALED until otherwise ordered by the Court. Specifically, disclosure of the requested order and investigation would likely result in flight from prosecution, a modification of the **Subject's** activities or the activities of those with whom **Subject** communicates and associates, or the destruction or tampering of evidence; and would otherwise seriously jeopardize the investigation.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief, and that this declaration was executed on **[DATE]**, at _____.

_____

[1]Any potential interference to service occasioned by use of the Pen Register or Trap and Trace will be minimized so as to be no more disruptive than might ordinarily occur with cellular service coverage.

[APPLICANT]
Assistant U.S. Attorney_____
[TELEPHONE NUMBER]

The following form is designed for the purpose of identifying an unknown phone – that is, a phone whose identifying attributes are not known – being used/carried by a known individual.

In brief, the technique involves using field equipment owned and operated by the law enforcement agency to detect all powered-on phones in the immediate vicinity of the subject. (Carrier assistance is not normally required unless the subject's location is unknown.) The survey is repeated at various times and in various locations, ideally at least 3 or 4, in proximity to the subject. The end product is a list of wireless instruments present and operating at each location, where the element common to those lists – typically a single device – represents the identifier for the subject's phone.

Because the objective is simply to identify the unknown device, collection should be limited to device identifiers (e.g., IMEI, IMSI, MIN, etc.). It should not encompass dialed digits, as that would entail surveillance on the calling activity of all persons in the vicinity of the subject. Once the subject's phone is identified, you may obtain a conventional pen/trap order or other legal process addressed to the relevant carrier.

Finally, note that a separate form – not this form – should be employed for using law enforcement field equipment to determine the unknown physical location of a known phone.

Questions or comments about this form or the underlying technique may be directed to

(b)(6)&(7)(C)
Associate Director
Office of Enforcement Operations
(b)(6)&(7)(C)
(b)(6)&(7)(C)

Rev. 1.3 8-11-08

UNITED STATES DISTRICT COURT
FOR THE [ ] DISTRICT OF [ ]
[ ] DIVISION

IN THE MATTER OF THE	§	
APPLICATION OF THE UNITED	§	
STATES OF AMERICA FOR AN	§	Case No. _____
ORDER AUTHORIZING THE	§	
INSTALLATION AND USE	§	(UNDER SEAL)
OF A PEN REGISTER AND TRAP	§	
AND TRACE DEVICE	§	

ORDER

This matter comes before the Court pursuant to written and sworn application under 18 U.S.C. §§ 3122(a)(1) and 3127(5) by Assistant United States Attorney **[Name]** (Applicant), an Attorney for the Government as defined by Federal Rule of Criminal Procedure Rule 1(b)(1)(B), applying for an order authorizing the use of a pen register and trap & trace device to identify the telephone number or other unique information (such as the Electronic Serial Number (ESN), International Mobile Equipment Identity (IMEI), or Mobile Equipment Identifier (MEID)) identifying the telephone (hereinafter the "Subject Telephone") being used by [SUBJECT'S NAME] in connection with an ongoing criminal investigation.

Pursuant to 18 U.S.C. § 3123(a)(1), Applicant has certified that the information likely to be obtained by the proposed pen register and trap and trace device is relevant to an ongoing criminal investigation being conducted by [**Investigative Agency**] regarding **[Offense Description, such as: 18 U.S.C. §))]** by **[SUBJECT'S NAME IN CAPS]** (Subject). The identity of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied is unknown. The order applies to the wireless telephone believed to be operated by the Subject to transmit wire or electronic communications. The pen register or trap and trace device is to be applied in the vicinity of the Subject to determine the number or other identifier of the Subject Telephone.

THEREFORE, IT IS HEREBY ORDERED, pursuant to 18 U.S.C. § 3123, that agents of

[**Investigative Agency**] may install and use a pen register and trap and trace device anywhere in the United States to record or decode the telephone number or other unique information (such as the Electronic Serial Number (ESN), International Mobile Equipment Identity (IMEI), or Mobile Equipment Identifier (MEID)) necessary to identify the Subject Telephone. [**Investigative agency**] shall neither retain nor make affirmative investigative use of data acquired beyond that necessary to identify the Subject telephone more fully.

IT IS FURTHER ORDERED THAT this Order shall be effective for sixty (60) days from the date this Order is signed by the court. 18 U.S.C. §§ 3123(c).

IT IS FURTHER ORDERED THAT , pursuant to 18 U.S.C. § 3123(d), that the Application and this Order are herewith SEALED until otherwise ordered by this Court.

Signed on _____ 2008, at_____.

_____

United States Magistrate Judge
[_____] District of [_____]

UNITED STATES DISTRICT COURT
FOR THE _____ DISTRICT OF _____

IN THE MATTER OF THE	§	
APPLICATION OF THE UNITED	§	
STATES OF AMERICA FOR AN	§	Case No. _____
ORDER AUTHORIZING THE	§	
INSTALLATION AND USE	§	(UNDER SEAL)
OF A PEN REGISTER AND TRAP	§	
AND TRACE DEVICE	§	

APPLICATION

The United States of America, by and through the undersigned Assistant United States Attorney, applies for an order authorizing the use of a pen register and trap & trace device to identify wireless telephone devices being used by persons suspected of committing federal crimes. In support of this application, Applicant states the following:

1. Applicant is an "attorney for the Government" as defined by Fed. R. Crim. P. 1(b)(1)(B) and, therefore, may apply for an order authorizing the installation and use of a pen register and trap & trace device. 18 U.S.C. §§ 3122(a)(1), 3127(5).

2. Applicant certifies that [**Investigative Agency**] is conducting an ongoing criminal investigation regarding **[Offense Description]** by **[SUBJECT'S NAME]** (hereafter, "**Subject**"), who is using one or more unidentified wireless telephones; and that **Subject** is known to live at or frequent the following locations: [Address1,] [Address2, etc]. The identity of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied is unknown. The order applies to wireless telephone communications utilizing GSM, CDMA, iDEN, TDMA, UMTS, or analog protocols—which comprise the entirety of all cellular or PCS wireless telephone protocols currently used in the United States. The number or other identifier of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied is unknown and it is the purpose of the requested order to identify this unknown information, such as the electronic serial number (ESN), international mobile equipment identity (IMEI), international

mobile subscriber identity (IMSI), or mobile equipment identifier (MEID).[1] The information likely to be obtained from the pen register and trap & trace device is relevant to the aforementioned investigation because it will enable investigators to identify **Subject's** phone. 18 U.S.C. § 3122(b)(1) & (2).

3. Pursuant to 18 U.S.C. § 3123(a)(1), Applicant requests the Court issue an order authorizing the installation and use of a pen register and trap and trace device for a period of sixty (60) days to detect radio signals emitted from wireless cellular telephones in the vicinity of the Subject that identify the telephones (e.g., by transmitting the telephone's serial number and phone number) to the network for authentication. By determining the identifying registration data at various locations in which the Subject Telephone is reasonably believed to be operating, the telephone number corresponding to the Subject Telephone can be identified. Data transmitted during autonomous registration is not dialed or otherwise controlled by the telephone user. It is an autonomous transmission that occurs when the phone is turned on and periodically thereafter, regardless of whether a call is being made, and in fact, is clearly separate from the establishment or maintenance of a call.

4. Applicant further requests that this application any order entered in connection therewith be SEALED until otherwise ordered by the Court. Specifically, disclosure of the requested order and investigation would likely result in flight from prosecution, a modification of the **Subject's** activities or the activities of those with whom **Subject** communicates and associates, or the destruction or tampering of evidence; and would otherwise seriously jeopardize the investigation.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief, and that this declaration was executed on **[DATE]**, at _____.

_____

[1]Any potential interference to service occasioned by use of the Pen Register or Trap and Trace will be minimized so as to be no more disruptive than might ordinarily occur with cellular service coverage.

[APPLICANT]
Assistant U.S. Attorney_____
[TELEPHONE NUMBER]

The following form is designed for the purpose of identifying an unknown phone – that is, a phone whose identifying attributes are not known – being used/carried by a known individual.

In brief, the technique involves using field equipment owned and operated by the law enforcement agency to detect all powered-on phones in the immediate vicinity of the subject. (Carrier assistance is not normally required unless the subject's location is unknown.) The survey is repeated at various times and in various locations, ideally at least 3 or 4, in proximity to the subject. The end product is a list of wireless instruments present and operating at each location, where the element common to those lists – typically a single device – represents the identifier for the subject's phone.

Because the objective is simply to identify the unknown device, collection should be limited to device identifiers (e.g., IMEI, IMSI, MIN, etc.). It should not encompass dialed digits, as that would entail surveillance on the calling activity of all persons in the vicinity of the subject. Once the subject's phone is identified, you may obtain a conventional pen/trap order or other legal process addressed to the relevant carrier.

Finally, note that a separate form – not this form – should be employed for using law enforcement field equipment to determine the unknown physical location of a known phone.

Questions or comments about this form or the underlying technique may be directed to

(b)(6)&(7)(C)
Associate Director
Office of Enforcement Operations
(b)(6)&(7)(C)
(b)(6)&(7)(C)

Rev. 1.3 8-11-08

UNITED STATES DISTRICT COURT
FOR THE [ ] DISTRICT OF [ ]
[ ] DIVISION

IN THE MATTER OF THE	§	
APPLICATION OF THE UNITED	§	
STATES OF AMERICA FOR AN	§	Case No. _____
ORDER AUTHORIZING THE	§	
INSTALLATION AND USE	§	(UNDER SEAL)
OF A PEN REGISTER AND TRAP	§	
AND TRACE DEVICE	§	

ORDER

This matter comes before the Court pursuant to written and sworn application under 18 U.S.C. §§ 3122(a)(1) and 3127(5) by Assistant United States Attorney **[Name]** (Applicant), an Attorney for the Government as defined by Federal Rule of Criminal Procedure Rule 1(b)(1)(B), applying for an order authorizing the use of a pen register and trap & trace device to identify the telephone number or other unique information (such as the Electronic Serial Number (ESN), International Mobile Equipment Identity (IMEI), or Mobile Equipment Identifier (MEID)) identifying the telephone (hereinafter the "Subject Telephone") being used by [SUBJECT'S NAME] in connection with an ongoing criminal investigation.

Pursuant to 18 U.S.C. § 3123(a)(1), Applicant has certified that the information likely to be obtained by the proposed pen register and trap and trace device is relevant to an ongoing criminal investigation being conducted by [**Investigative Agency**] regarding **[Offense Description, such as: 18 U.S.C. §))]** by **[SUBJECT'S NAME IN CAPS]** (Subject). The identity of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied is unknown. The order applies to the wireless telephone believed to be operated by the Subject to transmit wire or electronic communications. The pen register or trap and trace device is to be applied in the vicinity of the Subject to determine the number or other identifier of the Subject Telephone.

THEREFORE, IT IS HEREBY ORDERED, pursuant to 18 U.S.C. § 3123, that agents of

[**Investigative Agency**] may install and use a pen register and trap and trace device anywhere in the United States to record or decode the telephone number or other unique information (such as the Electronic Serial Number (ESN), International Mobile Equipment Identity (IMEI), or Mobile Equipment Identifier (MEID)) necessary to identify the Subject Telephone. [**Investigative agency**] shall neither retain nor make affirmative investigative use of data acquired beyond that necessary to identify the Subject telephone more fully.

IT IS FURTHER ORDERED THAT this Order shall be effective for sixty (60) days from the date this Order is signed by the court. 18 U.S.C. §§ 3123(c).

IT IS FURTHER ORDERED THAT , pursuant to 18 U.S.C. § 3123(d), that the Application and this Order are herewith SEALED until otherwise ordered by this Court.

Signed on _____ 2008, at_____.

_____

United States Magistrate Judge
[_____] District of [_____]

UNITED STATES DISTRICT COURT
FOR THE _____ DISTRICT OF _____

IN THE MATTER OF THE	§	
APPLICATION OF THE UNITED	§	
STATES OF AMERICA FOR AN	§	Case No. _____
ORDER AUTHORIZING THE	§	
INSTALLATION AND USE	§	(UNDER SEAL)
OF A PEN REGISTER AND TRAP	§	
AND TRACE DEVICE	§	

APPLICATION

The United States of America, by and through the undersigned Assistant United States Attorney, applies for an order authorizing the use of a pen register and trap & trace device to identify wireless telephone devices being used by persons suspected of committing federal crimes. In support of this application, Applicant states the following:

1. Applicant is an "attorney for the Government" as defined by Fed. R. Crim. P. 1(b)(1)(B) and, therefore, may apply for an order authorizing the installation and use of a pen register and trap & trace device. 18 U.S.C. §§ 3122(a)(1), 3127(5).

2. Applicant certifies that [**Investigative Agency**] is conducting an ongoing criminal investigation regarding **[Offense Description]** by **[SUBJECT'S NAME]** (hereafter, "**Subject**"), who is using one or more unidentified wireless telephones; and that **Subject** is known to live at or frequent the following locations: [Address1,] [Address2, etc]. The identity of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied is unknown. The order applies to wireless telephone communications utilizing GSM, CDMA, iDEN, TDMA, UMTS, or analog protocols—which comprise the entirety of all cellular or PCS wireless telephone protocols currently used in the United States. The number or other identifier of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied is unknown and it is the purpose of the requested order to identify this unknown information, such as the electronic serial number (ESN), international mobile equipment identity (IMEI), international

mobile subscriber identity (IMSI), or mobile equipment identifier (MEID).[1] The information likely to be obtained from the pen register and trap & trace device is relevant to the aforementioned investigation because it will enable investigators to identify **Subject's** phone. 18 U.S.C. § 3122(b)(1) & (2).

3. Pursuant to 18 U.S.C. § 3123(a)(1), Applicant requests the Court issue an order authorizing the installation and use of a pen register and trap and trace device for a period of sixty (60) days to detect radio signals emitted from wireless cellular telephones in the vicinity of the Subject that identify the telephones (e.g., by transmitting the telephone's serial number and phone number) to the network for authentication. By determining the identifying registration data at various locations in which the Subject Telephone is reasonably believed to be operating, the telephone number corresponding to the Subject Telephone can be identified. Data transmitted during autonomous registration is not dialed or otherwise controlled by the telephone user. It is an autonomous transmission that occurs when the phone is turned on and periodically thereafter, regardless of whether a call is being made, and in fact, is clearly separate from the establishment or maintenance of a call.

4. Applicant further requests that this application any order entered in connection therewith be SEALED until otherwise ordered by the Court. Specifically, disclosure of the requested order and investigation would likely result in flight from prosecution, a modification of the **Subject's** activities or the activities of those with whom **Subject** communicates and associates, or the destruction or tampering of evidence; and would otherwise seriously jeopardize the investigation.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief, and that this declaration was executed on **[DATE]**, at _____.

_____

[1]Any potential interference to service occasioned by use of the Pen Register or Trap and Trace will be minimized so as to be no more disruptive than might ordinarily occur with cellular service coverage.

[APPLICANT]
Assistant U.S. Attorney_____
[TELEPHONE NUMBER]

PROCEDURES FOR AUTHORIZING EMERGENCY INSTALLATION OF PEN REGISTER AND TRAP AND TRACE DEVICES ("PEN/TRAP") UNDER 18 U.S.C. 3125

I. **Justification:**

A. A situation where there is: 1) an immediate threat to life or limb; 2) a threat to national security; 3) activity characteristic of organized crime; or 4) an ongoing attack of a protected computer (one used by financial institution or U.S. government) where violation is a felony; AND

B. An order cannot be obtained with an exercise of due diligence, AND

C. There are grounds upon which an order could be issued (information sought is relevant to ongoing criminal activity).

II. **Procedures:**

A. Obtain the following, relevant facts: 1) circumstances giving rise to the emergency situation; 2) who, if known, is using the target phone/facility; 3) how the phone/facility was identified; 4) when the phone/facility was last known to be used; and 5) most recent criminal activity.

B. Call a Deputy Assistant Attorney General (DAAG), through the Command Center, at (b)(6)&(7)(C) .

C. Once approval has been obtained, call the law enforcement officer or AUSA back and advise them of the following: 1) an application and order must be filed within 48 hours (weekends and holidays included) after the installation of the equipment has occurred or begins to occur; and 2) the authorization obtained applies only to that specific phone/facility - the use of a pen/trap on any additional phones or facilities that may be identified during the emergency situation need to authorized by the DAAG.

III. **Consent:** If the request pertains to the victim's phone or a phone used by someone who is cooperating with the investigation, consider whether consent would apply. The cooperating party may consent to the installation of a trap and trace/pen register on their phone, and with respect to the victim, consent may be implied depending on the circumstances. See 18 U.S.C. 3121(b)(2)("user" may consent)

PROCEDURES FOR EMERGENCY REQUESTS FOR CELL SITE DATA WHEN SOUGHT IN CONNECTION WITH A PEN/TRAP

I. **Justification:** See above

II. **Procedures:** See above. When advising the AUSA or agent about filing the application and proposed order, instruct them to file an application that cites to both the pen register/trap and trace statute and 18 U.S.C. 2703(d).

III. **Invocation of 18 U.S.C. 2702(c)(4) to receive prospective cell site:** Reliance on this provision to allow repeated, perspective collection of cell site data may be problematic. Judicious use of this provision is advised. Advise the field that the more prudent course of action is to obtain a search warrant under Rule 41 for repeated disclosures of prospective cell site information because Rule 41 has prospective effect.

IV. **Consent:** As with an emergency pen/trap request, consider whether consent would apply. See 18 U.S.C. 2702(c)(2) - allowing a provider to disclose a record or other information with the consent of the "customer or subscriber."

* **NOTE:** A service provider can voluntarily disclose **historical** cell site data under 18 U.S.C. 2702(c)(4), and follow-up compulsory process is unnecessary.

PROCEDURES FOR EMERGENCY REQUESTS FOR LATITUDE/LONGITUDE DATA FOR CELLULAR PHONES, I.E., GPS, E-911, TOWER TRILATERATION

The Department cannot authorize the collection of GPS (latitude/longitude) data, E-911 information, or location information generated through tower trilateration under the emergency pen/trap statute. (Tower trilateration measures the signal strength from multiple cell towers to locate the phone and is relatively accurate.) If law enforcement seeks this information, they need to obtain a search warrant under Rule 41, absent an emergency or voluntary disclosure by the service provider. Again, consent is an option if the target phone belongs to the victim or someone cooperating with the investigation.

When advising the field, ascertain if the service provider can actually produce the information.

* Sprint/Nextel: True GPS

* T-Mobile: Tower trilateration

* Verizon Wireless/Alltel: no GPS, unless the phone is used to call 911. Typically, these providers can only pinpoint the location of a cell phone within the "banana range" from a cell tower.

In addition, GPS data can only be captured when the phone is on and registering with the network. Providers do not maintain historical GPS/E-911 data. One exception is the "kiddie tracker" phone service.

One final consideration is where to obtain the warrant. Obtain the warrant where the phone is reasonably believed to be.

PROCEDURES FOR EMERGENCY WIRETAP REQUESTS
PURSUANT TO 18 U.S.C. 2518(7)

I. Justification:

A. A situation where there is: 1) an immediate threat to life or limb; 2) conspiratorial activity characteristic of organized crime; or 3) conspiratorial activity threatening national security; AND

B. An order cannot be obtained with an exercise of due diligence; AND

C. There are grounds upon which an order could be issued, i.e. probable cause for a predicate offense and/or federal felony (usually not an issue) and legal necessity.

II. Procedures:

A. Obtain the following, relevant facts: 1) circumstances giving rise to the emergency situation; 2) who, if known, is using the target phone/facility/location; 3) how the target phone/facility/location was identified; 4) when the phone/facility/location was last known to be used; 5) most recent criminal activity; and 6) basis for belief that phone/facility/location will be used for communications concerning the crime, i.e. what evidence is there that the perpetrator is acting in concert with others - what communications will be obtained.

B. Call a DAAG, through the Command Center, at (b)(6)&(7)(C) (b)(6)&(7)(C) and advise the official of the facts.

C. Once the DAAG concurs that an emergency situation exists, call the law enforcement officer or AUSA back and advise them of the following: 1) the Criminal Division agrees that an emergency tap may be sought; 2) the law enforcement officer must proceed up his chain of command to seek approval for the emergency tap; and 3) a high-level official of the law enforcement agency (for example, the Assistant Director or Director of the FBI) must contact either the AG, the DAG, or the AAG (Associate Attorney General) to obtain approval to proceed with the emergency tap.

D. Once the tap has been authorized by DOJ, the AUSA must file an application, affidavit, and proposed order within 48 hours after the interception has occurred or begins to occur. (Sample pleadings are available on USABook).

E. The affidavit in support of the emergency must contain only those facts known to the law enforcement officer at the time the emergency authorization was obtained from DOJ.

F. All pleadings must be reviewed by OEO before the AUSA goes to court.

G. Any documentation of the emergency authorization would come from the law enforcement agency and would include the date and time of the authorization, the identity of the authorizing official, and a description of the phone/facility/location that was authorized for interception, i.e., the phone number for the phone, the email address for the internet account, or the physical address of the location. This documentation should be filed with the AUSA's application. OEO/Criminal Division does not provide such documentation as we are not involved directly with the approval process at the AG/DAG/AAG level.

H. Continued surveillance: If the law enforcement agency wants to extend interceptions beyond the first 48-hour period, then:

1. They must seek DAAG authority to do so.

2. The affidavit filed in support of the emergency request may also include a section that provides probable cause to extend the interceptions. The affidavit must clearly differentiate between those facts in support of the emergency and those in support of the extension request.

3. Separate applications and orders should be filed for the emergency and extension requests.

USE OF WITT EQUIPMENT

WITT is a catchall term for equipment that law enforcement can use to locate a cellular phone. It includes devices called Wolfpack, Stingray, and Gossamer. WITT equipment emulates a cell phone tower and can be used to determine which direction the phone is in and how strong the signal is.

If law enforcement seeks to use their WITT equipment to locate a cellular phone, they need to obtain a pen register and trap and trace order for that phone. If they want to use the WITT equipment in an emergency situation, they must obtain DOJ approval first. Consent, for the reasons stated herein, may also apply.

The following form is designed for the purpose of identifying an unknown phone – that is, a phone whose identifying attributes are not known – being used/carried by a known individual.

In brief, the technique involves using field equipment owned and operated by the law enforcement agency to detect all powered-on phones in the immediate vicinity of the subject. (Carrier assistance is not normally required unless the subject's location is unknown.) The survey is repeated at various times and in various locations, ideally at least 3 or 4, in proximity to the subject. The end product is a list of wireless instruments present and operating at each location, where the element common to those lists – typically a single device – represents the identifier for the subject's phone.

Because the objective is simply to identify the unknown device, collection should be limited to device identifiers (e.g., IMEI, IMSI, MIN, etc.). It should not encompass dialed digits, as that would entail surveillance on the calling activity of all persons in the vicinity of the subject. Once the subject's phone is identified, you may obtain a conventional pen/trap order or other legal process addressed to the relevant carrier.

Finally, note that a separate form – not this form – should be employed for using law enforcement field equipment to determine the unknown physical location of a known phone.

Questions or comments about this form or the underlying technique may be directed to

(b)(6)&(7)(C)
Associate Director
Office of Enforcement Operations
(b)(6)&(7)(C)
(b)(6)&(7)(C)

Rev. 1.3 8-11-08

UNITED STATES DISTRICT COURT
FOR THE [ ] DISTRICT OF [ ]
[ ] DIVISION

IN THE MATTER OF THE	§	
APPLICATION OF THE UNITED	§	
STATES OF AMERICA FOR AN	§	Case No. _____
ORDER AUTHORIZING THE	§	
INSTALLATION AND USE	§	(UNDER SEAL)
OF A PEN REGISTER AND TRAP	§	
AND TRACE DEVICE	§	

ORDER

This matter comes before the Court pursuant to written and sworn application under 18 U.S.C. §§ 3122(a)(1) and 3127(5) by Assistant United States Attorney **[Name]** (Applicant), an Attorney for the Government as defined by Federal Rule of Criminal Procedure Rule 1(b)(1)(B), applying for an order authorizing the use of a pen register and trap & trace device to identify the telephone number or other unique information (such as the Electronic Serial Number (ESN), International Mobile Equipment Identity (IMEI), or Mobile Equipment Identifier (MEID)) identifying the telephone (hereinafter the "Subject Telephone") being used by [SUBJECT'S NAME] in connection with an ongoing criminal investigation.

Pursuant to 18 U.S.C. § 3123(a)(1), Applicant has certified that the information likely to be obtained by the proposed pen register and trap and trace device is relevant to an ongoing criminal investigation being conducted by [**Investigative Agency**] regarding **[Offense Description, such as: 18 U.S.C. §))]** by **[SUBJECT'S NAME IN CAPS]** (Subject). The identity of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied is unknown. The order applies to the wireless telephone believed to be operated by the Subject to transmit wire or electronic communications. The pen register or trap and trace device is to be applied in the vicinity of the Subject to determine the number or other identifier of the Subject Telephone.

THEREFORE, IT IS HEREBY ORDERED, pursuant to 18 U.S.C. § 3123, that agents of

[**Investigative Agency**] may install and use a pen register and trap and trace device anywhere in the United States to record or decode the telephone number or other unique information (such as the Electronic Serial Number (ESN), International Mobile Equipment Identity (IMEI), or Mobile Equipment Identifier (MEID)) necessary to identify the Subject Telephone. [**Investigative agency**] shall neither retain nor make affirmative investigative use of data acquired beyond that necessary to identify the Subject telephone more fully.

IT IS FURTHER ORDERED THAT this Order shall be effective for sixty (60) days from the date this Order is signed by the court. 18 U.S.C. §§ 3123(c).

IT IS FURTHER ORDERED THAT , pursuant to 18 U.S.C. § 3123(d), that the Application and this Order are herewith SEALED until otherwise ordered by this Court.

Signed on _____ 2008, at_____.

_____

United States Magistrate Judge
[_____] District of [_____]

UNITED STATES DISTRICT COURT
FOR THE _____ DISTRICT OF _____

IN THE MATTER OF THE	§	
APPLICATION OF THE UNITED	§	
STATES OF AMERICA FOR AN	§	Case No. _____
ORDER AUTHORIZING THE	§	
INSTALLATION AND USE	§	(UNDER SEAL)
OF A PEN REGISTER AND TRAP	§	
AND TRACE DEVICE	§	

APPLICATION

The United States of America, by and through the undersigned Assistant United States Attorney, applies for an order authorizing the use of a pen register and trap & trace device to identify wireless telephone devices being used by persons suspected of committing federal crimes. In support of this application, Applicant states the following:

1. Applicant is an "attorney for the Government" as defined by Fed. R. Crim. P. 1(b)(1)(B) and, therefore, may apply for an order authorizing the installation and use of a pen register and trap & trace device. 18 U.S.C. §§ 3122(a)(1), 3127(5).

2. Applicant certifies that [**Investigative Agency**] is conducting an ongoing criminal investigation regarding **[Offense Description]** by **[SUBJECT'S NAME]** (hereafter, "**Subject**"), who is using one or more unidentified wireless telephones; and that **Subject** is known to live at or frequent the following locations: [Address1,] [Address2, etc]. The identity of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied is unknown. The order applies to wireless telephone communications utilizing GSM, CDMA, iDEN, TDMA, UMTS, or analog protocols—which comprise the entirety of all cellular or PCS wireless telephone protocols currently used in the United States. The number or other identifier of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied is unknown and it is the purpose of the requested order to identify this unknown information, such as the electronic serial number (ESN), international mobile equipment identity (IMEI), international

mobile subscriber identity (IMSI), or mobile equipment identifier (MEID).[1] The information likely to be obtained from the pen register and trap & trace device is relevant to the aforementioned investigation because it will enable investigators to identify **Subject's** phone. 18 U.S.C. § 3122(b)(1) & (2).

3. Pursuant to 18 U.S.C. § 3123(a)(1), Applicant requests the Court issue an order authorizing the installation and use of a pen register and trap and trace device for a period of sixty (60) days to detect radio signals emitted from wireless cellular telephones in the vicinity of the Subject that identify the telephones (e.g., by transmitting the telephone's serial number and phone number) to the network for authentication. By determining the identifying registration data at various locations in which the Subject Telephone is reasonably believed to be operating, the telephone number corresponding to the Subject Telephone can be identified. Data transmitted during autonomous registration is not dialed or otherwise controlled by the telephone user. It is an autonomous transmission that occurs when the phone is turned on and periodically thereafter, regardless of whether a call is being made, and in fact, is clearly separate from the establishment or maintenance of a call.

4. Applicant further requests that this application any order entered in connection therewith be SEALED until otherwise ordered by the Court. Specifically, disclosure of the requested order and investigation would likely result in flight from prosecution, a modification of the **Subject's** activities or the activities of those with whom **Subject** communicates and associates, or the destruction or tampering of evidence; and would otherwise seriously jeopardize the investigation.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief, and that this declaration was executed on **[DATE]**, at _____.

_____

[1]Any potential interference to service occasioned by use of the Pen Register or Trap and Trace will be minimized so as to be no more disruptive than might ordinarily occur with cellular service coverage.

[APPLICANT]
Assistant U.S. Attorney_____
[TELEPHONE NUMBER]