ATTACHED EXHIBITS
RESPONSE TO GOVERNMENT'S MEMORANDUM REGARDING LAW ENFORCEMENT PRIVILEGE
AND REQUEST FOR AN EX PARTE AND IN CAMERA HEARING IF NECESSARY
CR08-814-PHX-DGC

↓ **EXHIBIT 31** ↓
↓ **EXHIBIT 31** ↓
↓ **EXHIBIT 31** ↓
↓ **EXHIBIT 31** ↓
↓ **EXHIBIT 31** ↓
↓ **EXHIBIT 31** ↓
↓ **EXHIBIT 31** ↓
↓ **EXHIBIT 31** ↓
↓ **EXHIBIT 31** ↓
↓ **EXHIBIT 31** ↓
↓ **EXHIBIT 31** ↓
↓ **EXHIBIT 31** ↓
↓ **EXHIBIT 31** ↓
↓ **EXHIBIT 31** ↓
↓ **EXHIBIT 31** ↓
↓ **EXHIBIT 31** ↓
↓ **EXHIBIT 31** ↓
↓ **EXHIBIT 31** ↓
↓ **EXHIBIT 31** ↓
↓ **EXHIBIT 31** ↓
↓ **EXHIBIT 31** ↓
↓ **EXHIBIT 31** ↓
↓ **EXHIBIT 31** ↓
↓ **EXHIBIT 31** ↓
↓ **EXHIBIT 31** ↓
↓ **EXHIBIT 31** ↓
↓ **EXHIBIT 31** ↓
↓ **EXHIBIT 31** ↓
↓ **EXHIBIT 31** ↓
↓ **EXHIBIT 31** ↓
↓ **EXHIBIT 31** ↓
↓ **EXHIBIT 31** ↓

McPherson, Rodney, *et al.* (Palm Bay FL, US), Harris Corp., U.S. Patent No. 7,592,956 [Wireless Transmitter Location Determining System And Related Methods] (Sep. 22, 2009), *available at* <http://www.freepatentsonline.com/7592956.html> (last accessed Feb. 22, 2011);

US007592956B2

(12) **United States Patent**
McPherson et al.

(10) **Patent No.: US 7,592,956 B2**
(45) **Date of Patent: Sep. 22, 2009**

(54) **WIRELESS TRANSMITTER LOCATION DETERMINING SYSTEM AND RELATED METHODS**

(75) Inventors: **Rodney Keith McPherson**, Palm Bay, FL (US); **David James Lanza**, Indian Harbour Beach, FL (US)

(73) Assignee: **Harris Corporation**, Melbourne, FL (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **12/029,689**

(22) Filed: **Feb. 12, 2008**

(65) **Prior Publication Data**

US 2009/0201208 A1 Aug. 13, 2009

(51) **Int. Cl.**
G01S 3/02 (2006.01)

(52) **U.S. Cl.** **342/458**; 342/457

(58) **Field of Classification Search** 342/357.06, 342/442, 457, 458, 463–465; 455/456.1, 455/456.3, 457

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,343,212	A *	8/1994	Rose et al.	342/424
5,526,001	A *	6/1996	Rose et al.	342/442
5,719,584	A	2/1998	Otto	342/465
5,890,068	A	3/1999	Fattouche et al.	455/456
5,914,687	A	6/1999	Rose	342/442
5,974,039	A	10/1999	Schilling	370/335
6,054,950	A	4/2000	Fontana	342/463
6,233,459	B1	5/2001	Sullivan	455/456
6,249,252	B1	6/2001	Dupray	342/450
6,407,703	B1	6/2002	Minter et al.	342/450
6,765,533	B2	7/2004	Szajnowski	342/465
6,882,315	B2	4/2005	Richley et al.	342/465
7,057,556	B2	6/2006	Hall et al.	342/387
7,187,327	B2	3/2007	Coluzzi et al.	342/458
7,203,497	B2	4/2007	Belcea	455/446
7,203,500	B2	4/2007	Leeper et al.	455/456.1
2003/0112183	A1	6/2003	Szajnowski	342/465
2004/0029558	A1	2/2004	Liu	455/414.3
2006/0087475	A1 *	4/2006	Struckman	342/451
2006/0267841	A1 *	11/2006	Lee et al.	342/463
2007/0247367	A1	10/2007	Anjum et al.	342/464
2008/0161015	A1 *	7/2008	Maloney et al.	455/456.1

FOREIGN PATENT DOCUMENTS

WO	97/28456	8/1997
WO	2007/124300	11/2007

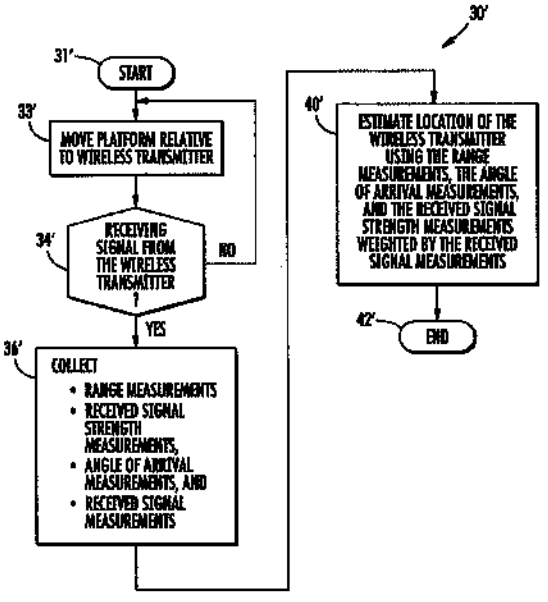
* cited by examiner

Primary Examiner—Dao L Phan
(74) *Attorney, Agent, or Firm*—Allen, Dyer, Doppelt, Milbrath & Gilchrist, P.A.

(57) **ABSTRACT**

A location determining system for a wireless transmitter is carried by a platform movable relative to the wireless transmitter. The location determining system may include an antenna, and a receiver coupled to the antenna. The location determining system may also include a location determining processor coupled to the receiver to collect, during movement relative to the wireless transmitter, a series of range measurements and a corresponding series of received signal measurements, and to estimate a location of the wireless transmitter based upon the range measurements weighted using the received signal measurements.

21 Claims, 10 Drawing Sheets



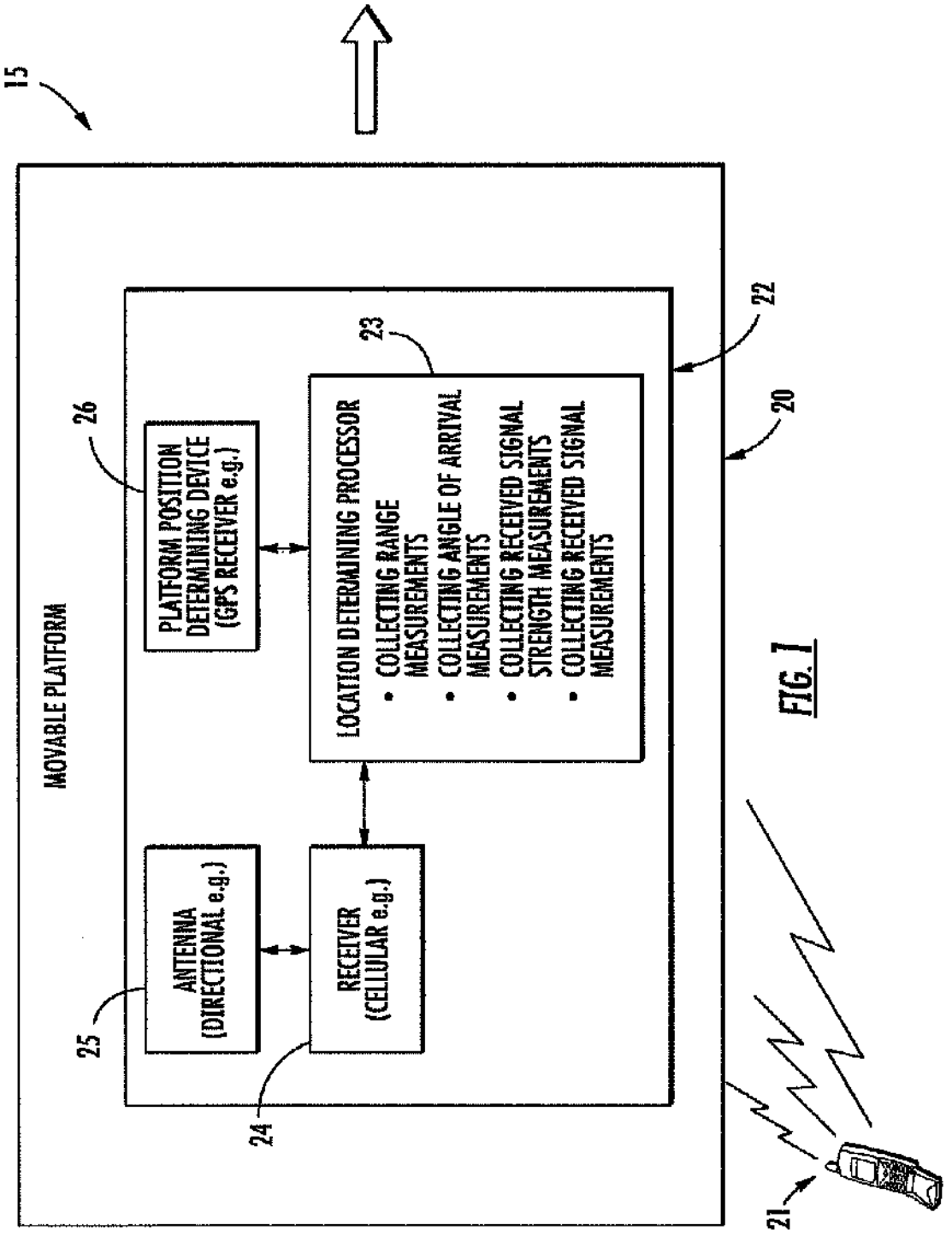

15
MOVABLE PLATFORM
PLATFORM POSITION DETERMINING DEVICE (GPS RECEIVER e.g.)
26
LOCATION DETERMINING PROCESSOR
• COLLECTING RANGE MEASUREMENTS
• COLLECTING ANGLE OF ARRIVAL MEASUREMENTS
• COLLECTING RECEIVED SIGNAL STRENGTH MEASUREMENTS
• COLLECTING RECEIVED SIGNAL MEASUREMENTS
23
22
20
ANTENNA (DIRECTIONAL e.g.)
25
RECEIVER (CELLULAR e.g.)
24
21

FIG. 1

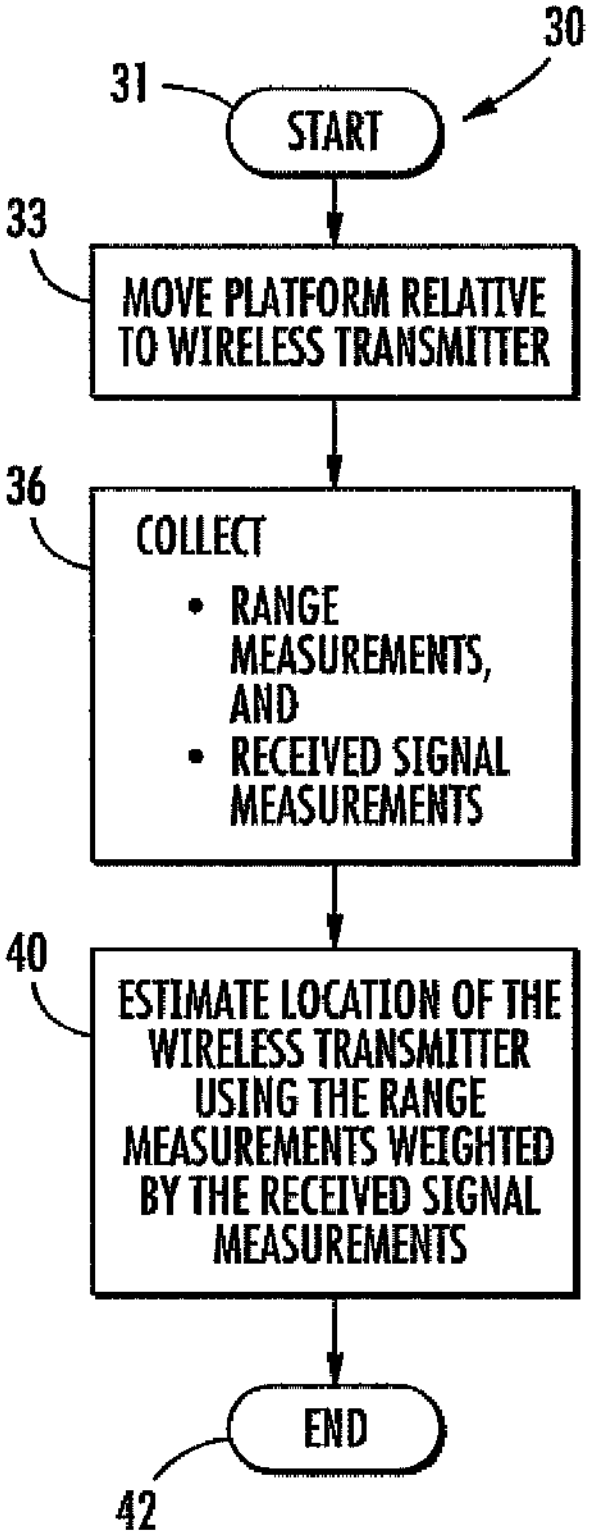

30
31
START
33
MOVE PLATFORM RELATIVE TO WIRELESS TRANSMITTER
36
COLLECT
• RANGE MEASUREMENTS, AND
• RECEIVED SIGNAL MEASUREMENTS
40
ESTIMATE LOCATION OF THE WIRELESS TRANSMITTER USING THE RANGE MEASUREMENTS WEIGHTED BY THE RECEIVED SIGNAL MEASUREMENTS
END
42

FIG. 2

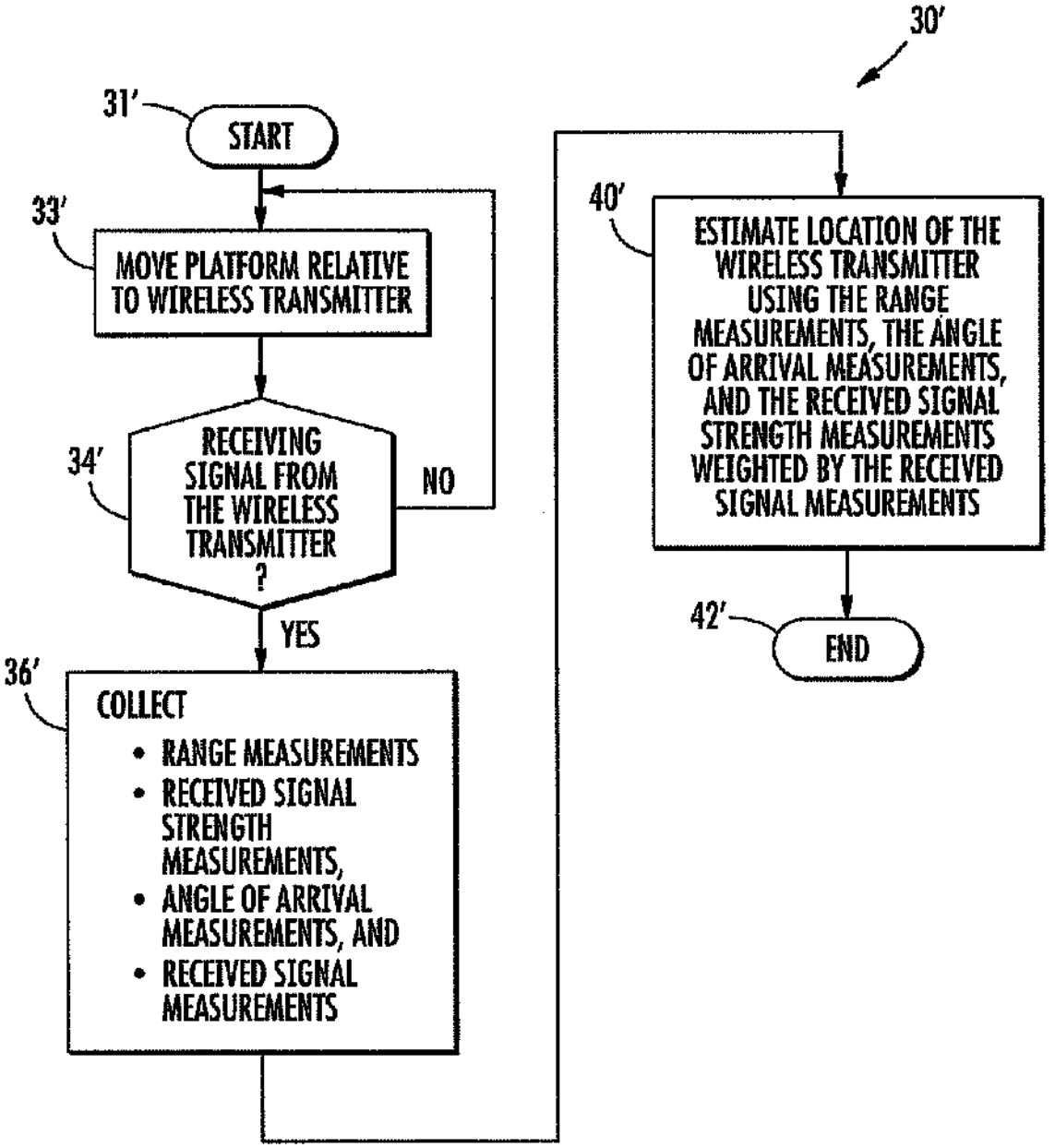

30'
31'
START
33'
MOVE PLATFORM RELATIVE TO WIRELESS TRANSMITTER
34'
RECEIVING SIGNAL FROM THE WIRELESS TRANSMITTER ?
NO
YES
36'
COLLECT
• RANGE MEASUREMENTS
• RECEIVED SIGNAL STRENGTH MEASUREMENTS,
• ANGLE OF ARRIVAL MEASUREMENTS, AND
• RECEIVED SIGNAL MEASUREMENTS
40'
ESTIMATE LOCATION OF THE WIRELESS TRANSMITTER USING THE RANGE MEASUREMENTS, THE ANGLE OF ARRIVAL MEASUREMENTS, AND THE RECEIVED SIGNAL STRENGTH MEASUREMENTS WEIGHTED BY THE RECEIVED SIGNAL MEASUREMENTS
42'
END

FIG. 3

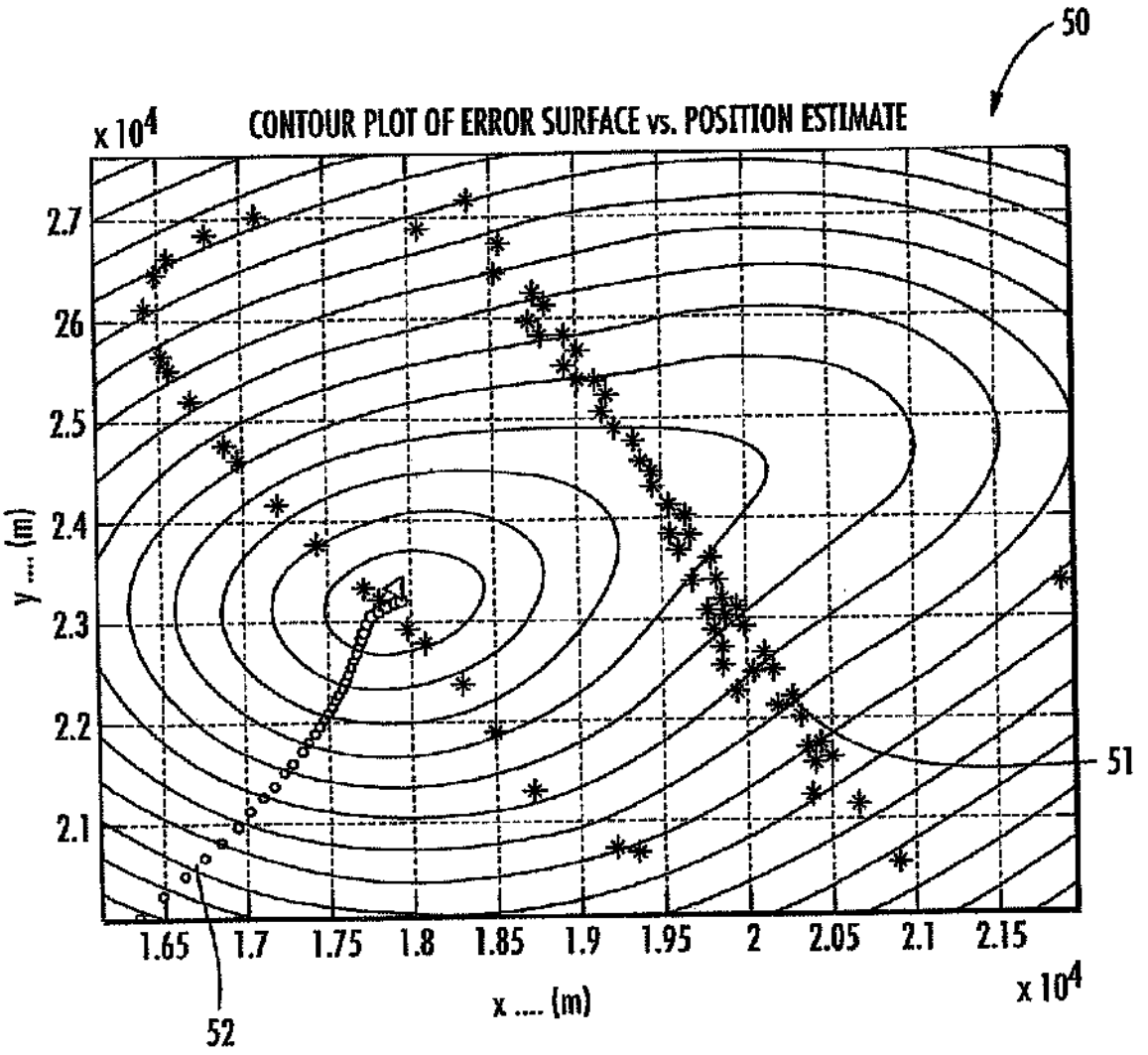

50
CONTOUR PLOT OF ERROR SURFACE vs. POSITION ESTIMATE
x 10^4
2.7
2.6
2.5
2.4
2.3
2.2
2.1
y .... (m)
1.65
1.7
1.75
1.8
1.85
1.9
1.95
2
2.05
2.1
2.15
x .... (m)
x 10^4
51
52

FIG. 4

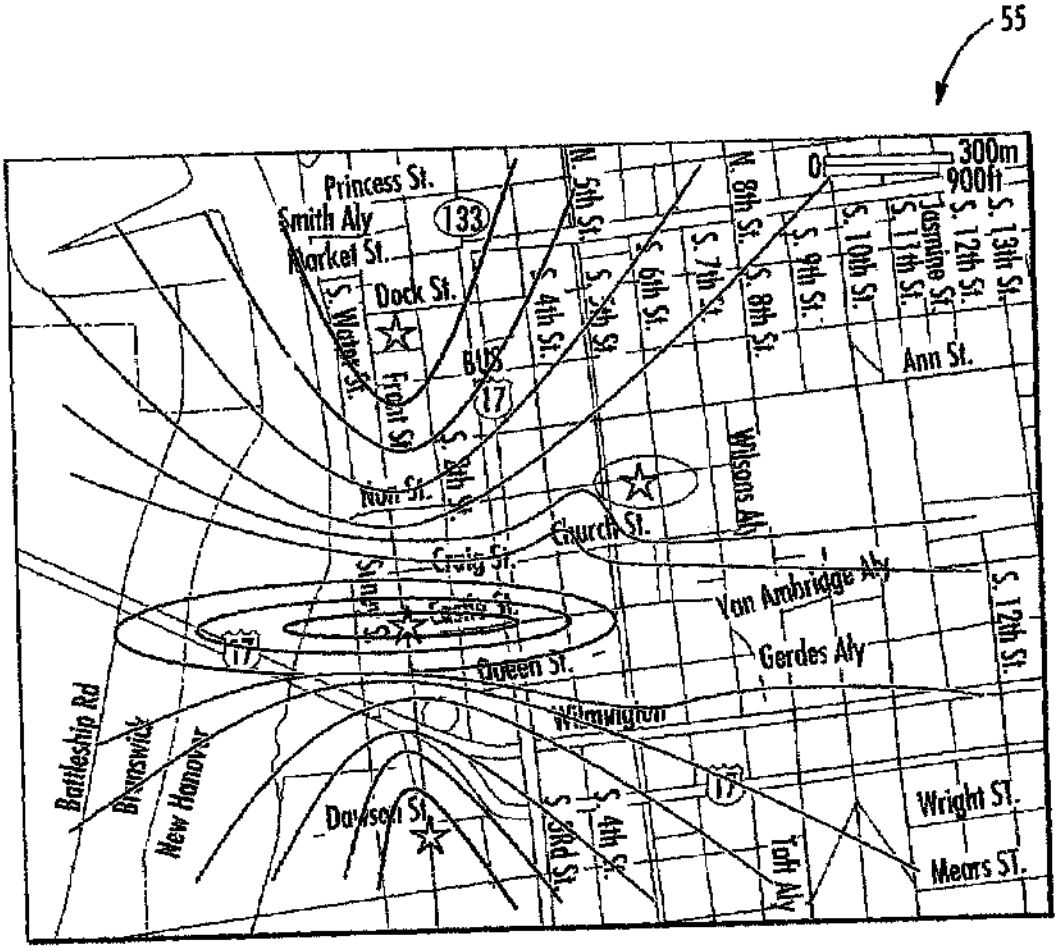

55
300m
900ft
Princess St.
Smith Aly
Market St.
Dock St.
S. Water St.
Front St.
133
BUS
17
N. 5th St.
S. 4th St.
S. 5th St.
S. 6th St.
S. 7th St.
N. 8th St.
S. 8th St.
S. 9th St.
S. 10th St.
S. 11th St.
Jasmine St.
S. 12th St.
S. 13th St.
Ann St.
Wilsons Aly
Church St.
Craig St.
Van Ambridge Aly
Gerdes Aly
Queen St.
Wilmington
Battleship Rd
Brunswick
New Hanover
Davidson St.
S. 3rd St.
S. 4th St.
Taft Aly
Wright ST.
Mears ST.

FIG. 5

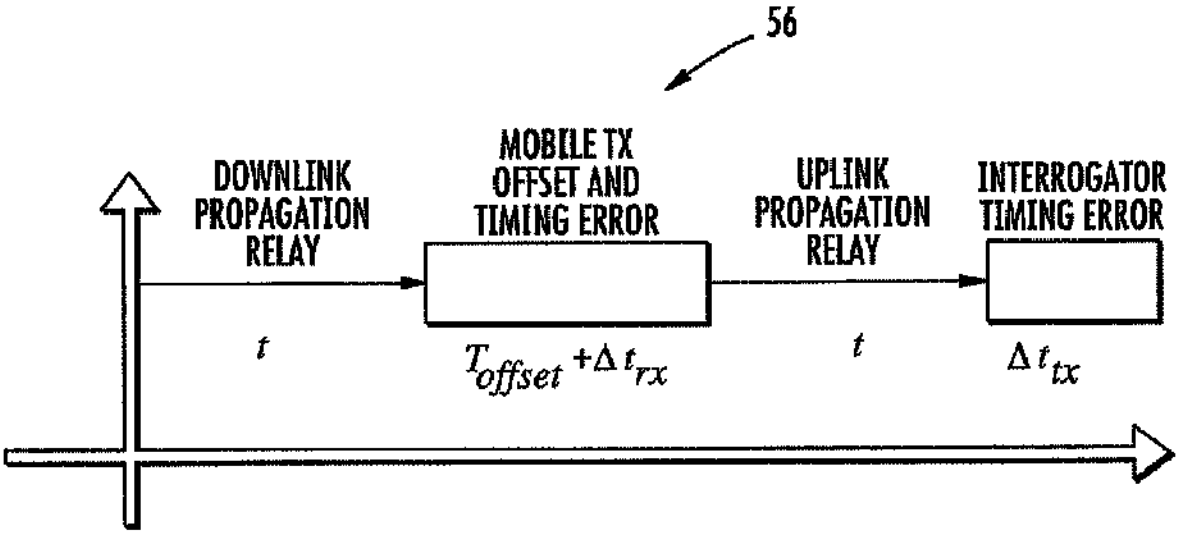

56
DOWNLINK PROPAGATION RELAY
MOBILE TX OFFSET AND TIMING ERROR
UPLINK PROPAGATION RELAY
INTERROGATOR TIMING ERROR
t
$T_{offset} + \Delta t_{rx}$
t
Δt_{tx}

FIG. 6

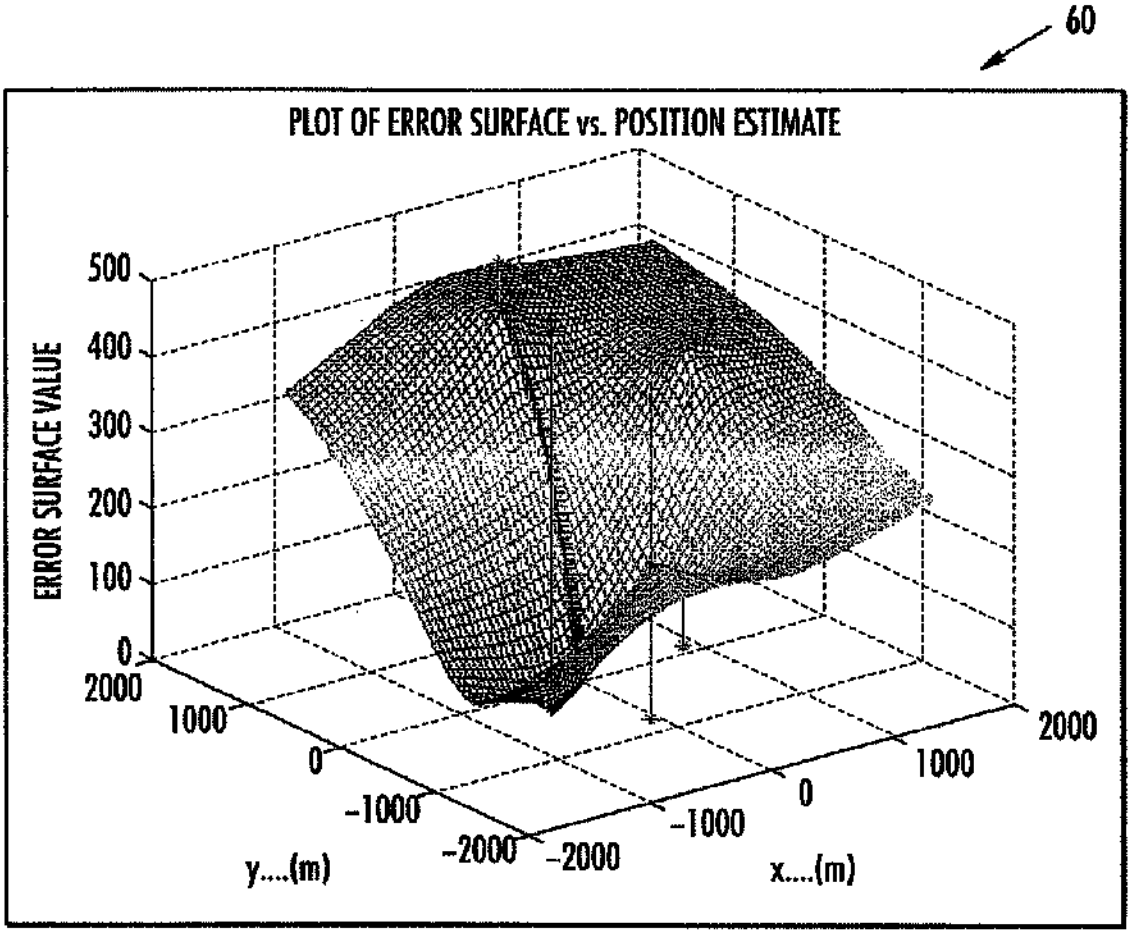

60
PLOT OF ERROR SURFACE vs. POSITION ESTIMATE
ERROR SURFACE VALUE
500
400
300
200
100
0
2000
1000
0
-1000
-2000
y....(m)
-2000
-1000
0
1000
2000
x....(m)

FIG. 7

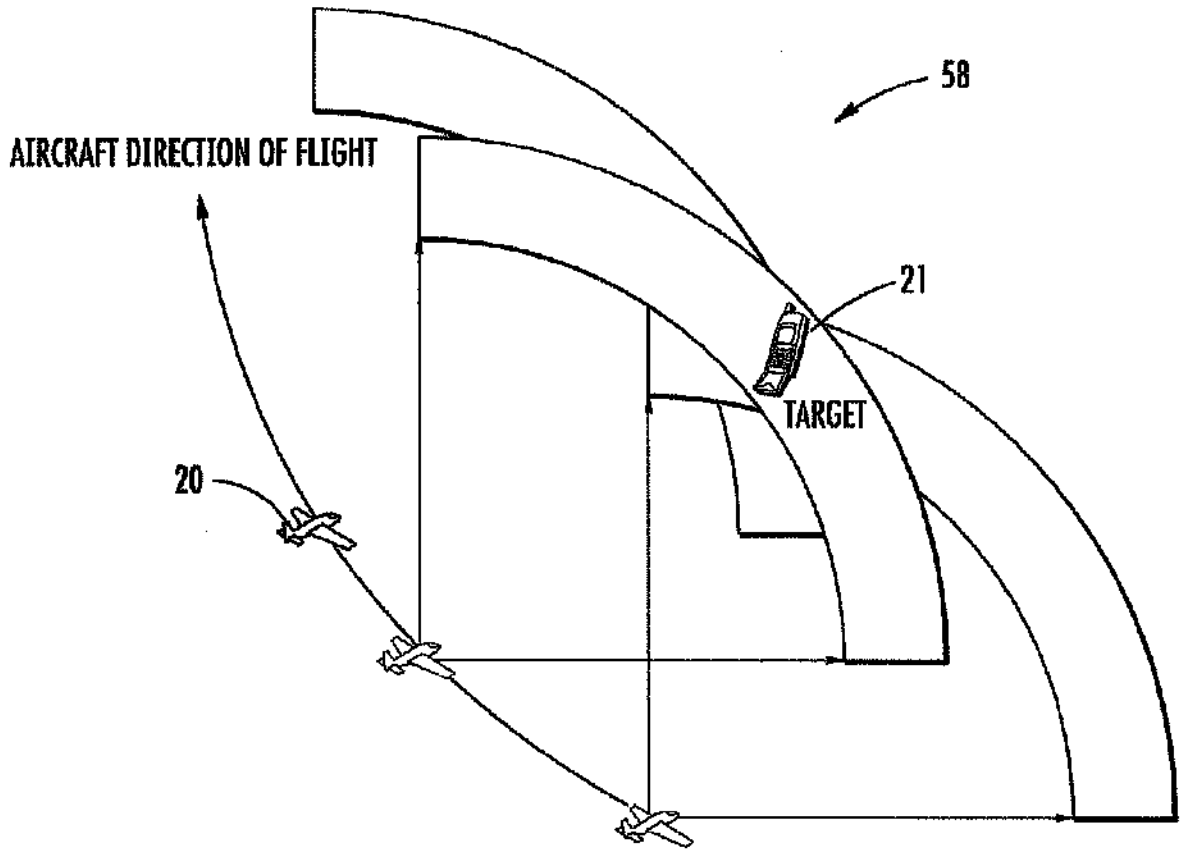


FIG. 8

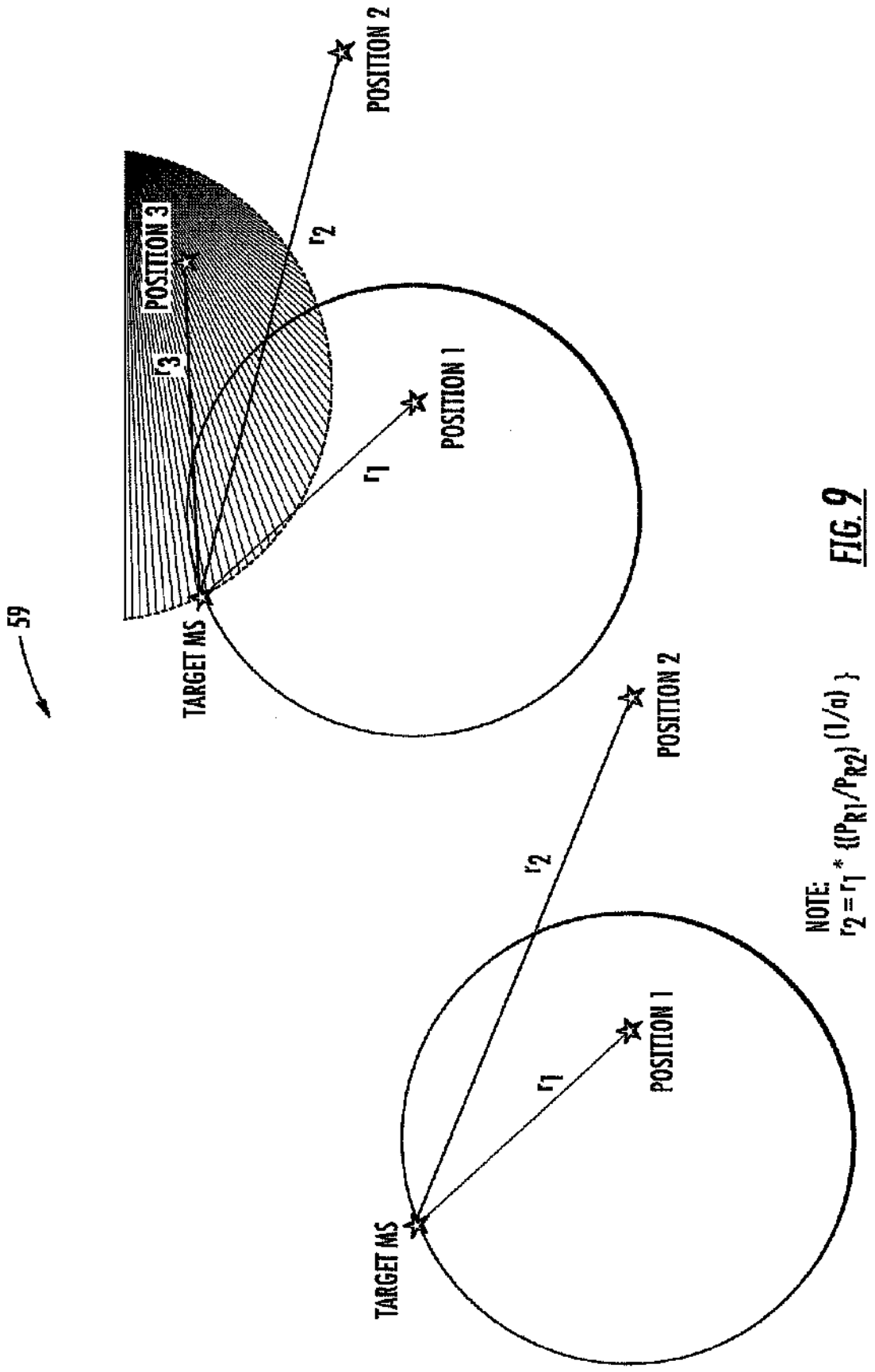

59
TARGET MS
POSITION 1
POSITION 2
POSITION 3
r1
r2
r3
TARGET MS
POSITION 1
POSITION 2
r1
r2
NOTE:
r2 = r1 * {(PR1/PR2) (1/α) }

FIG. 9

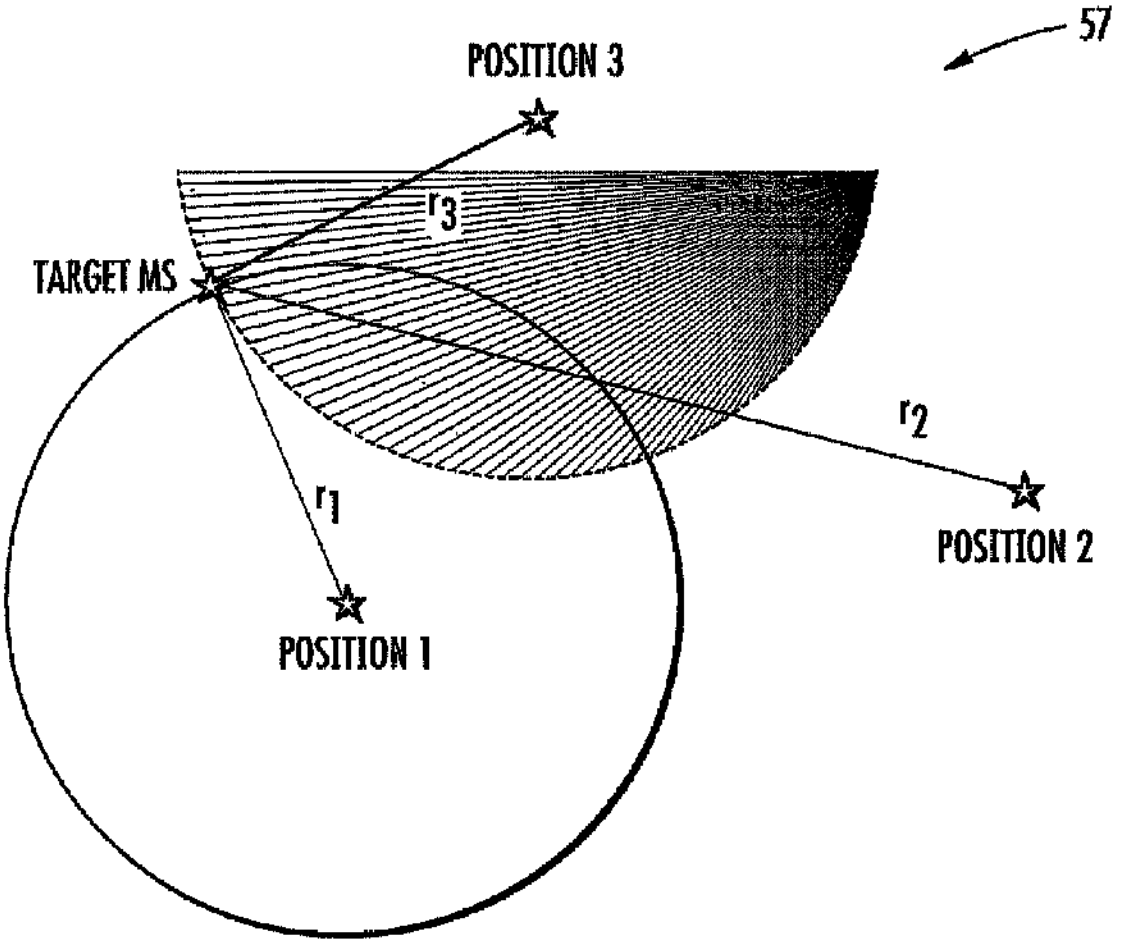


FIG. 10

WIRELESS TRANSMITTER LOCATION DETERMINING SYSTEM AND RELATED METHODS

FIELD OF THE INVENTION

The present invention relates to the field of wireless transmission, and, more particularly, to a location determining system for a wireless transmitter and related methods.

BACKGROUND OF THE INVENTION

As cellular communication has become prevalent, it is not uncommon for a person to carry a cellular telephone device with them on a daily basis. Because of this, there is desire by local police and fire departments to use a corresponding cellular telephone device to help locate a missing person, for example, a person trapped in a collapsed building or a fugitive. Conventional approaches to cellular telephone device location include systems comprising a plurality of sensors. These systems typically use a triangulation method to determine the location of the cellular telephone device.

One approach to cellular telephone device location is disclosed by U.S. Pat. No. 6,407,703 to Minter et al. The system of Minter et al. includes a plurality of sensors situated in multiple locations/platforms. The system uses angle of arrival (AOA), time difference of arrival (TDOA), and terrain altitude information from signal intercepts from the cellular telephone device to determine the location thereof. The sensors use accurate time synchronization for determining the TDOA of the intercepted signals

Another approach to locating a cellular telephone device is disclosed in U.S. Pat. No. 7,187,327 to Coluzzi et al. This system also includes a plurality of sensors using TDOA and time of arrival measurements of signals received from the cellular telephone device to determine the location thereof. The sensors in this system are also synchronized.

Another approach to locating a cellular telephone device is disclosed in U.S. Pat. No. 7,203,500 to Leeper et al. This system uses a wireless transceiver device to determine range to a companion wireless transceiver device, for example, the cellular telephone device, with signal propagation time measurements. Another approach to locating a cellular telephone device is disclosed in U.S. Pat. No. 7,057,556 to Hall et al. This system includes a plurality of sensors also using TDOA to determine the location of the cellular telephone device.

Another approach is disclosed in U.S. Pat. No. 5,719,584 to Otto, assigned to the present application's assignee, Harris Corporation of Melbourne, Fla. This system uses a plurality of ground based sensors to determine a location of the cellular telephone device by measuring TDOA and AOA values. This network of sensors is also synchronized.

An approach to locating a cellular telephone device within a high-rise structure is disclosed in U.S. Pat. No. 7,203,497 to Belcea. This system includes a plurality of sensors deployed throughout the structure that use signal propagation time measurements to determine the approximate location of the cellular telephone device within the structure.

The prior art systems for location of cellular telephone devices may suffer from several drawbacks. For example, these systems use multiple sensors that are synchronized for generation of TDOA measurements. The systems are also complex and expensive, and require multiple sensors on different platforms. The systems also provide inaccurate location data if the sensors are not properly deployed.

SUMMARY OF THE INVENTION

In view of the foregoing background, it is therefore an object of the present invention to provide a location determining system for a wireless transmitter that is accurate and less complex.

This and other objects, features, and advantages in accordance with the present invention are provided by a location determining system for a wireless transmitter, the location determining system to be carried by a platform movable relative to the wireless transmitter. The location determining system may include an antenna, and a receiver coupled to the antenna. The location determining system may also include a location determining processor coupled to the receiver to collect, during movement relative to the wireless transmitter, a series of range measurements and a corresponding series of received signal measurements, and to estimate a location of the wireless transmitter based upon the range measurements weighted using the received signal measurements. Advantageously, the location determining system is simpler and less costly to deploy.

For example, the received signal measurements may comprise at least one of bit-error rate measurements, received signal strength measurements, receiver metrics, and signal-to-noise ratio measurements. Additionally, the location determining processor may further estimate an elevation of the wireless transmitter. The location determining processor may estimate the location of the wireless transmitter based upon a least-squares steepest decent algorithm.

The location determining system may also comprise a platform position determining device. The location determining processor may cooperate with the platform position determining device so that the estimated location of the wireless transmitter comprises an estimated geolocation. The location determining processor may collect the series of range measurements using time of flight measurements.

In certain embodiments, the antenna may comprise a directional antenna. In these embodiments, the location determining processor may cooperate with the directional antenna to collect, during movement relative to the wireless transmitter, a corresponding series of angle of arrival measurements. The location determining processor may also estimate the location of the wireless transmitter further based upon the angle of arrival measurements. Furthermore, the location determining processor may weight the angle of arrival measurements based upon the received signal measurements. In some embodiments, the platform may comprise an aircraft. Alternatively, the platform may comprise a ground-based vehicle.

Moreover, the location determining processor may cooperate with the receiver to collect, during movement relative to the wireless transmitter, a corresponding series of received signal strength measurements. The location determining processor may further estimate the location of the wireless transmitter further based upon the received signal strength measurements weighted using the received signal measurements.

Another aspect is directed to a method of estimating a location of a wireless transmitter using a location determining system. The method may comprise collecting, during movement of the location determining system relative to the wireless transmitter, a series of range measurements and a corresponding series of received signal measurements. The method may also include estimating a location of the wireless transmitter based upon the range measurements weighted using the received signal measurements.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a schematic diagram of a location determining system, according to the present invention, being carried by a movable platform.

FIG. **2** is a flowchart illustrating a method of estimating a location of a wireless transmitter using the location determining system, according to the present invention.

FIG. **3** is a more detailed flowchart of the method of estimating a location of a wireless transmitter using the location determining system, according to the present invention.

FIG. **4** is a contour plot of an error surface for a test run of the location determining system, according to the present invention.

FIG. **5** is an exemplary contour plot of an error surface for the location determining system, according to the present invention, superimposed on a map of the geographical terrain.

FIG. **6** is a chart illustrating the process for establishing frame boundaries with a wireless transmitter in the location determining system, according to the present invention.

FIG. **7** is an exemplary three-dimensional contour plot of an error surface for the location determining system, according to the present invention.

FIG. **8** is a schematic diagram of the location determining system, according to the present invention, receiving signals from the wireless transmitter.

FIG. **9** is a schematic diagram of the location determining system, according to the present invention, estimating the location of the wireless transmitter.

FIG. **10** is a second schematic diagram of the location determining system, according to the present invention, estimating the location of the wireless transmitter.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention will now be described more fully hereinafter with reference to the accompanying drawings, in which preferred embodiments of the invention are shown. This invention may, however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein. Rather, these embodiments are provided so that this disclosure will be thorough and complete, and will fully convey the scope of the invention to those skilled in the art. Like numbers refer to like elements throughout, and prime notation is used to indicate similar elements in alternative embodiments.

Referring initially to FIG. **1**, a communication system **15** illustratively includes a location determining system **22** and a wireless transmitter **21**. The location determining system **22** is illustratively carried by a platform **20** movable relative to the wireless transmitter **21**. The platform **20** may comprise an airborne platform, for example, an aircraft, or alternatively a ground based vehicle platform, for example, an automobile. As will be appreciated by those skilled in the art, the effective range of the location determining system **22** may increase in embodiments including the airborne platform.

The wireless transmitter **21** illustratively comprises a cellular telephone. The receiver **24** may comprise a receiver compatible with the cellular telephone. As will be appreciated by those skilled in the art, the cellular telephone may be compatible with the Global System for Mobile communications (GSM) standard, the code division multiple access (CDMA) standard, the IS-95 standard, the CDMA2000 standard, or the UMTS mobile telephone standard.

The location determining system **22** illustratively includes an antenna **25**, and a receiver **24** coupled to the antenna. The location determining system **22** illustratively includes a location determining processor **23** coupled to the receiver **24** to collect, during movement relative to the wireless transmitter **21**, a series of range measurements and a corresponding series of received signal measurements, and to estimate a location of the wireless transmitter based upon the range measurements weighted using the received signal measurements. For example, the range measurements may comprise time of flight measurements, i.e. the time elapsed for a transmission signal to traverse the distance between the platform **20** and the wireless transmitter **21**. Advantageously, the location determining system **22** includes a single sensor/antenna **25** for determining the location of the wireless transmitter **21**. Accordingly, no synchronization or alignment of the sensors may be needed in some embodiments.

The received signal measurements may comprise, for example, at least one of bit-error rate measurements, received signal strength measurements, receiver metrics (i.e. Viterbi path metrics), and signal-to-noise ratio measurements. In other words, the received signal measurements relate directly to the quality of the signal being received by the location determining system **22**.

Referring briefly to FIG. **6**, the time of flight measurements may be based upon the following equation.

$$\underset{Estimated}{T_{elapse}} = 2t_0 + \underset{known}{T_{offset}} + \overbrace{\underset{Bound}{\Delta t_{rx}} + \underset{Bound}{\Delta t_{tx}}}^{Error\ Terms}$$

The distance between the wireless transmitter **21** and the platform **20** may be provided by the following equation.

$$\hat{d} = c\left[\frac{T_{elapse} - T_{offset}}{2}\right] = d + c\left[\frac{\Delta t_{rx} + \Delta t_{tx}}{2}\right]$$

More specifically, and as depicted in the diagram **56** of FIG. **6**, the antenna **25** may transmit a signal to be received by the wireless transmitter **21**. As will be appreciated by those skilled in the art, the signal may comprise a signal that would routinely prompt a transmission reply from the wireless transmitter **21** under the applicable communication standard. Once the wireless transmitter **21** receives the signal from the location determining system **22**, the wireless transmitter transmits a reply signal that is received by the platform **20**. As will be appreciated by those skilled in the art, the location determining system **22** may compensate for the mobile transmitter **21** transmission delay, i.e. processing lag (T_{offset}) before transmission of a reply signal to the platform **20**. In some embodiments, the receiver **24** may comprise a transceiver for transmitting the signal to the wireless transmitter **21**.

In other embodiments, the time of flight measurements may be generated using a time of transmission stamp within the reply signal by differing the reply signal receipt time with the indicated time of transmission. As will be appreciated by those skilled in the art, the platform **20** and the wireless transmitter **21** may be time synced via satellite, for example, the Global Positioning System.

In certain embodiments, the antenna **25** may comprise a directional antenna, for example, a switched beam antenna. In these embodiments, the location determining processor **23** cooperates with the directional antenna to collect, during movement relative to the wireless transmitter **21**, a corre-

sponding series of angle of arrival measurements. The location determining processor **23** estimates the location of the wireless transmitter **21** further based upon the angle of arrival measurements. Furthermore, the location determining processor **23** weights the angle of arrival measurements based upon the received signal measurements, for example, at least one of bit-error rate measurements, received signal strength measurements, receiver metrics, and signal-to-noise ratio measurements.

In other embodiments, the location determining processor **23** may cooperate with the receiver **24** to collect, during movement relative to the wireless transmitter **21**, a corresponding series of received signal strength measurements. The location determining processor **23** may estimate the location of the wireless transmitter **21** further based upon the received signal strength measurements weighted using the received signal measurements, for example, at least one of bit-error rate measurements, received signal strength measurements, receiver metrics, and signal-to-noise ratio measurements. The location determining processor **23** may use the received signal strength measurements for breaking the symmetry, ambiguity resolution, etc. In other words, the location determining processor **23** may weight the received signal strength measurements based upon the bit-error rate, for example. In alternative embodiments, the weighting of the received signal strength measurements may also comprise, for example, a unity factor (no weighting).

As the platform **20** moves relative to the wireless transmitter **21**, this motion is shown in the diagram **58** of FIG. **8**, the location determining processor **23** generates a series of range-bearings equations. As discussed above, each range-bearing equation is based upon at least the range measurements and the received signal measurements but may also include the AOA measurements and the received signal strength measurements. The range-bearing equations may be solved to provide an estimated location of the wireless transmitter **21**. As will be appreciated by those skilled in the art, the time elapsed between generation of each range-bearing equation is based upon platform **20** velocity and the type of platform.

Referring briefly to FIG. **4**, a contour plot **50** of an error surface for a test run of the location determining system **22** is illustrated. The light grey star points **51** represent the position of the platform **20** as it moves relative to the wireless transmitter **21**. The dark grey points **52** represent the iterative, estimated solutions of the series of range-bearing equations, the points moving toward the actual location of the wireless transmitter **21** as they become more accurate. The contour plot of the error surface provides an approximate error of the estimated location of the wireless transmitter **21** based upon the locations of the platform **20**. The contour plot **50** may assist a user of the platform **20** (for example, aircraft or ground vehicle) in determining the distribution of errors based upon the geometry, therefore allowing for the optimization of the ground search for the wireless transmitter **21**. As will be appreciated by those skilled in the art, FIG. **7** includes an exemplary three-dimensional error contour plot **60**.

Referring again to FIG. **1**, the location determining processor **23** may estimate the location of the wireless transmitter **21** based upon the range measurements, the angle of arrival measurements, and the received signal strength measurements weighted by the received signal measurements, for example, at least one of bit-error rate measurements, received signal strength measurements, receiver metrics, and signal-to-noise ratio measurements. More specifically, when the received signal measurement indicates a high quality received signal, for example, when the signal-to-noise ratio value is larger, the location determining processor **23** interprets the other associated signal measurements (range measurements, AOA measurements, received signal strength measurements) relevant to the estimation of the wireless transmitter's **21** location to be of a higher quality, and therefore those measurements are more heavily weighted among the total set of measurements relevant to produce the location estimate.

As will be appreciated by those skilled in the art, the accuracy of the location estimate of the wireless transmitter **21**, which is based upon the range measurements, the AOA measurements, and the received signal strength measurements, varies based upon the overall geometry of the situation. As the platform **20** moves relative to the wireless transmitter **21**, the accuracy of the location estimate improves if the trajectory of the platform: breaks symmetry with regards to the wireless transmitter, reduces ambiguity resolution, and minimizes geometric dilution of precision (GDOP).

Hence, as the platform **20** moves relative to the wireless transmitter **21** and generates a series of range-bearing equations, the location determining processor **23** may give greater weight to range-bearing equations that correspond to positions with received signal measurements indicating a greater quality level. Moreover, the weighting between the range measurements, the received signal strength measurements, and the AOA measurements may be based upon a predetermined ratio that is based upon at least past experimental results.

The location determining system **22** illustratively includes a platform position determining device **26**, for example, a Global Positioning System (GPS) receiver. The platform position determining device **26** provides the location determining system **22** with a current geographic location of the platform **20**. The location determining processor **23** cooperates with the platform position determining device **26** so that the estimated location of the wireless transmitter **21** comprises an estimated geolocation. In other words, the location determining system **22** provides the estimated longitude and latitude of the wireless transmitter **21**. Additionally, the location determining processor **23** estimates an elevation of the wireless transmitter **21**, i.e. the altitude of the wireless transmitter. Advantageously, the error contour plot for the estimated location of the wireless transmitter **21** may be superimposed over a map **55** for advantageous reliability and search, example shown in FIG. **5**.

Referring now both to FIGS. **1** and **2**, a flowchart **30** illustrates a method of estimating a location of a wireless transmitter **21** using a location determining system **22**. At Block **31**, the method begins and illustratively includes moving at Block **33** the platform relative to the wireless transmitter **21**. As will be appreciated by those skilled in the art, it may be preferable to encircle the approximate location of the wireless transmitter **21** to provide more accurate results, i.e. breaking the symmetry.

The method illustratively includes at Block **36** collecting, during movement of the location determining system **22** relative to the wireless transmitter **21**, a series of range measurements and a corresponding series of received signal measurements. The method also illustratively includes estimating at Block **40** a location of the wireless transmitter **21** based upon the range measurements weighted using the received signal measurements, ending at Block **42**.

Referring now additionally to FIG. **3**, another embodiment of the method is now described. In this embodiment of the method, those elements already discussed above with respect to FIG. **2** are given prime notation and most require no further discussion herein. This embodiment differs from the previous embodiment in that the method further comprises a decision

Block **34'** for determining whether a transmission signal is received from the wireless transmitter **21**. If no signal is received, the method returns to Block **33'** and continues to move the platform **20** until the transmission signal is received. If the transmission signal is received, the method moves on to Block **36'** for collection of measurements. In this embodiment, at Block **36'**, the method further includes collecting corresponding angle of arrival measurements and corresponding received signal strength measurements. Moreover, at Block **40'**, the method further includes using angle of arrival measurements and received signal strength measurements weighted by the received signal measurements to estimate the location of the wireless transmitter **21**. The method ends at Block **42'**.

The location determining processor **23** estimates the location of the wireless transmitter **21** based upon a least-squares steepest decent algorithm. As will be appreciated by those skilled in the art, a detailed exemplary implementation of the mathematical algorithm used by the location determining system **22** of FIG. **1** follows.

The mathematical algorithm includes a Non-Linear Least Squares Steepest Descent Algorithm (NLSSDA) in a full 3D geolocation context using a variety of families of range equations. The algorithm may be applicable for ground level, elevated, or airborne sensors (or a combination thereof). The algorithm may function with a number of networked ground based sensors or a single mobile sensor (ground based or airborne) to accomplish target location estimation. The algorithm, itself rather decoupled from the specific measurement techniques, also works for a broad range of wireless signals, including GSM, IS-95, cdma2000, and UMTS, for example.

Section 1: Introduction

The following description derives and presents the relevant mathematics that apply to the 3D geolocation problem. Note that the various range equations and cost functions derived herein can be weighted and combined into the same adaptive algorithm, providing a viable data fusion technique to incorporate various families of data useful for the location estimation problem. Indeed, the algorithm may allow for the various measurements and families of measurements to be weighted relative to each other, such that, location estimate is optimized in a weighted least-squares sense.

The equations below are derived for the general case where the target is located in a 3D space, which may be useful if the target (wireless transmitter **21**) is in a high-rise building, in a mountainous region, or some similar situation. As will be appreciated by those skilled in the art, the specific case where the target is confined to ground level (i.e. z=0) is a special case and is readily dealt with using the more general equations. The specific coordinate system used is not relevant, and the algorithm has been demonstrated to operate quite effectively in an earth-centered-earth-fixed (ECEF) 3D coordinate system, for example. As will be appreciated by those skilled in the art, other coordinate systems may be used.

Section 2: Time of Flight Based Approach

The primary geolocation method is referred to as the time of flight (TOF) method. The following measurement cost function can be defined for the TOF method:

$$f_i(x) = \sqrt{(x_i - x)^2 + (y_i - y)^2 + (z_i - z)^2} - \frac{c\Delta t_i}{2}, \quad (1)$$

where

-continued

$$\Delta t_i = T^i_{elapse} - 3 \cdot T_{slots} + TA, \quad (2)$$

and

$$x = [x_0 y_0 z_0]^T.$$

As will be appreciated by those skilled in the art, equation (2) relates specifically to the GSM standard and may be modified to comply with other wireless standards. The terms in equation (2) are either known or measured, and the remaining terms in (1) depend only on the current positions of the sensor and the target estimate. In one embodiment, Δt_i=TA and location estimation is based on the reported timing advance (TA). In equations (1) and (2), the measurements are taken with the sensor (antenna **25**) at position i, and the unknown target position at position x. The following overall cost function can be defined over a set of measurements $i \in [1 \ldots N]$.

$$F(x) = \sum_{i=1}^{N} \alpha_i^2 f_i^2(x) \quad (3)$$

In equation (3), the α_i is a weighting term and can be set to establish the relative importance and/or quality of the measurements. This is the term that may be related to the signal quality estimate. The position estimate of the target can be updated according to the equation

$$x_{k+1} = x_k - U \nabla_x F(x_k), \quad (4)$$

where U is a diagonal matrix, where the algorithm convergence properties are controlled by the values of the diagonal elements, and

$$\nabla_x F(x_k) = \nabla_x F(x)|_{x_k} = \begin{pmatrix} \frac{\delta F}{\delta x}\Big|_{x_k} \\ \frac{\delta F}{\delta y}\Big|_{y_k} \\ \frac{\delta F}{\delta z}\Big|_{z_k} \end{pmatrix}. \quad (5)$$

It follows that the partial derivatives may be derived, which are used in equation (5). This may be done in the following development.

Let $u_i=(x_i-x)^2+(y_i-y)^2+(z_i-z)^2$, then rewrite formula (I) as

$$f_i(x) = \sqrt{u_i} - \frac{c\Delta t_i}{2}. \quad (6)$$

Now using differential Calculus, the partial derivative of the overall cost function in formula (3) is

$$\frac{\delta F}{\delta x} = 2 \cdot \sum_{i=1}^{n} \alpha_i^2 f_i(x) \cdot \frac{\delta f_i(x)}{\delta x}, \text{ where} \quad (7)$$

$$\frac{\delta f_i(x)}{\delta x} = \frac{1}{2\sqrt{u_i}} \cdot \frac{\delta u_i}{\delta x} = \frac{1}{2\sqrt{u_i}} \cdot 2(x_i - x) \cdot (-1) = \frac{(x - x_i)}{\sqrt{(x_i - x)^2 + (y_i - y)^2 + (z_i - z)^2}}. \quad (8)$$

The final form of the equation may be written as

$$\frac{\delta F}{\delta x}\Big|_{x_k} = 2 \cdot \sum_{i=1}^{N} \alpha_i^2 f_i(x) \cdot \frac{(x_k - x_i)}{\sqrt{(x_i - x_k)^2 + (y_i - y_k)^2 + (z_i - z_k)^2}}. \quad (9)$$

In like fashion, the other partial derivatives functions can be derived and are summarized below.

$$\frac{\delta F}{\delta y}\Big|_{y_k} = 2 \cdot \sum_{i=1}^{N} \alpha_i^2 f_i(x) \cdot \frac{(y_k - y_i)}{\sqrt{(x_i - x_k)^2 + (y_i - y_k)^2 + (z_i - z_k)^2}} \quad (10)$$

$$\frac{\delta F}{\delta z}\Big|_{z_k} = 2 \cdot \sum_{i=1}^{N} \alpha_i^2 f_i(x) \cdot \frac{(z_k - z_i)}{\sqrt{(x_i - x_k)^2 + (y_i - y_k)^2 + (z_i - z_k)^2}} \quad (11)$$

In summary, the NLSSDA for the TOF method is described by equations (4), (5), and (9)-(11).

Section 3: Received Signal Strength Indication Based Approach

This section derives the equations that use signal power measurements at multiple locations as a way to gain location information of the target. The derivation of the equations is included below in summary form. The measured target signal power at two locations can be used to write the following equations, where a is the path loss exponent, P_{RX} is the measured signal power, and r_x is the range.

$$r_2/r_1 = (P_{r1}/P_{r2})^{1/\alpha} \quad (12)$$

$$(r_2/r_1)^{\alpha} = (P_{r1}/P_{r2}) \quad (13)$$

$$(r_1/r_2)^{\alpha} = (P_{r2}/P_{r1}) \quad (14)$$

$$(r_i/r_{i+1})^{\alpha} = (P_{i+1}/P_i) \quad (15)$$

Now, after taking the log of both sides of (15), and expressing the ranges in terms of the relevant x, y, z coordinates, the following cost function is provided.

$$g_i(x) = \frac{P_{i+1}}{P_i} - \left\{ \frac{\sqrt{(x_i - x)^2 + (y_i - y)^2 + (z_i - z)^2}}{\sqrt{(x_{i+1} - x)^2 + (y_{i+1} - y)^2 + (z_{i+1} - z)^2}} \right\}^{\alpha}. \quad (16)$$

The relevant measurement cost function is expressed as

$$f_{RSSI}^i(x) = \log_{10} g_i(x) = P_{i+1}(dB) - P_i(dB) - \alpha \left\{ \log_{10} \sqrt{(x_i - x)^2 + (y_i - y)^2 + (z_i - z)^2} - \log_{10} \sqrt{(x_{i+1} - x)^2 + (y_{i+1} - y)^2 + (z_{i+1} - z)^2} \right\} \quad (17)$$

where again, $x=[x_0 y_0 z_0]^T$ is the current estimated position of the target.

The overall cost function is as described in equation (3), where $f_i(x)$ is replaced with $f_{RSSI}^i(x)$. The derivation of the partial derivatives for the measurement cost function in equation (17) makes use of the following form:

$$\frac{d}{dx} \log_a u = \log_a e \cdot \frac{1}{u} \cdot \frac{du}{dx}. \quad (18)$$

Applying equation (18) to equation (17), consider the following development. Let $u_i=(x_i-x)^2+(y_i-y)^2+(z_i-z)^2$, it can then be written as:

$$\frac{\delta f_{RSSI}^i(x)}{\delta x} = -\alpha \left\{ \log_{10} e \frac{1}{\sqrt{u_i}} \cdot \frac{1}{2\sqrt{u_i}} \cdot 2(x_i - x) \cdot (-1) - \log_{10} e \frac{1}{\sqrt{u_{i+1}}} \cdot \frac{1}{2\sqrt{u_{i+1}}} \cdot 2(x_{i+1} - x) \cdot (-1) \right\} \quad (19)$$

$$\frac{\delta f_{RSSI}^i(x)}{\delta x} = -\alpha \cdot \log_{10} e \cdot \left\{ \frac{(x - x_i)}{u_i} - \frac{(x - x_{i+1})}{u_{i+1}} \right\} \quad (20)$$

$$\frac{\delta f_{RSSI}^i(x)}{\delta y} = -\alpha \cdot \log_{10} e \cdot \left\{ \frac{(y - y_i)}{u_i} - \frac{(y - y_{i+1})}{u_{i+1}} \right\} \quad (21)$$

$$\frac{\delta f_{RSSI}^i(x)}{\delta z} = -\alpha \cdot \log_{10} e \cdot \left\{ \frac{(z - z_i)}{u_i} - \frac{(z - z_{i+1})}{u_{i+1}} \right\}. \quad (22)$$

Now using differential Calculus, the partial derivative of the overall cost function in equation (3) can be written as (recall general development in section 2):

$$\frac{\delta F}{\delta x}\Big|_{x_k} = 2 \cdot \sum_{i=1}^{N} \alpha_i^2 f_{RSSI}^i(x) \cdot \left(-\alpha \cdot \log_{10} e \cdot \left\{ \frac{(x_k - x_i)}{u_i} - \frac{(x_k - x_{i+1})}{u_{i+1}} \right\} \right) \quad (23)$$

$$\frac{\delta F}{\delta y}\Big|_{y_k} = 2 \cdot \sum_{i=1}^{N} \alpha_i^2 f_{RSSI}^i(x) \cdot \left(-\alpha \cdot \log_{10} e \cdot \left\{ \frac{(y_k - y_i)}{u_i} - \frac{(y_k - y_{i+1})}{u_{i+1}} \right\} \right) \quad (24)$$

$$\frac{\delta F}{\delta z}\Big|_{z_k} = 2 \cdot \sum_{i=1}^{N} \alpha_i^2 f_{RSSI}^i(x) \cdot \left(-\alpha \cdot \log_{10} e \cdot \left\{ \frac{(z_k - z_i)}{u_i} - \frac{(z_k - z_{i+1})}{u_{i+1}} \right\} \right). \quad (25)$$

In summary, the NLSSDA for the relative received signal strength indication (RSSI) method is described by equations (4), (5), and (23)-(25).

Referring to FIGS. **9-10**, charts **57**, **59** illustrate takings of the received signal strength measurements at N points, each pair of measurements may permit the construction of a circle. The target location is estimated as the intersection of the circles.

Section 4: Angle of Arrival Approach

This section derives the equations that use any AOA measurements that may be available at multiple locations as a way to gain location information of the target. These AOA measurements may be made, for example, with the aid of a switched beam antenna **25**. In like fashion, the other partial derivative functions can be derived and are summarized below.

This method is derived for 3D space, however, this may be optimal only if the antenna is highly directional in terms of azimuth and elevation. Indeed, practical antennas are most likely not highly directional in either orientation, however, even low resolution directivity information (used with low weights in the algorithm) may be useful for ambiguity resolution and breaking symmetry in the overall error surface. In the 3D case, it is assumed that the antenna is somewhat directional in terms of azimuth and elevation. The 2D case for antenna directivity may allow azimuth to be easily derived from the equations as a special case.

The derivation of the equations is included below in summary form. The sensor at each position i determines an estimated azimuth and elevation angle to the target. All angles are processed with knowledge of each sensor's measurement position and orientation so that the angles can be converted to a set of linear equations in the relevant 3D Cartesian coordinate system. There will be an equation for each sensor angle measurement. The final set of equations can be written as follows for each sensor i:

$$h_i(x)=z=m_i x+n_i y+b_i. \tag{26}$$

The relevant measurement cost function is expressed as

$$f_{ANG}^{\ i}(x)=m_i x+n_i y+b_i-z, \tag{27}$$

where again $x=[x_0 y_0 z_0]^T$ is the current estimated position of the target.

The overall cost function is as described in equation (3), where $f_i(x)$ is replaced with $f_{ANG}^{\ i}(x)$. The partial derivatives for the measurement cost function in equation (27) are easily established as:

$$\frac{\delta f_{ANG}^{i}(x)}{\delta x}=m_i \tag{28}$$

$$\frac{\delta f_{ANG}^{i}(x)}{\delta y}=n_i \tag{29}$$

$$\frac{\delta f_{ANG}^{i}(x)}{\delta z}=-1. \tag{30}$$

Now using differential Calculus, the partial derivative of the overall cost function in equation (3) can be written as (recall general development in section 2):

$$\frac{\delta F}{\delta x}\Big|_{x_k}=2\cdot\sum_{i=1}^{N}\alpha_i^2 f_{ANG}^{i}(x)\cdot m_i \tag{31}$$

$$\frac{\delta F}{\delta y}\Big|_{y_k}=2\cdot\sum_{i=1}^{N}\alpha_i^2 f_{ANG}^{i}(x)\cdot n_i \tag{32}$$

$$\frac{\delta F}{\delta z}\Big|_{z_k}=2\cdot\sum_{i=1}^{N}\alpha_i^2 f_{ANG}^{i}(x)\cdot(-1). \tag{33}$$

In summary, the NLSSDA for the relative RSSI method is described by equations (4), (5), and (31)-(33).

Section 5: Synchronized TDOA Approach

For completeness, an embodiment using the synchronized TDOA approach is also discussed herein, which is applicable for a set of time synchronized sensors. This section derives the synchronized TDOA equations, which use measurements at multiple locations as a way to gain location information of the target. Assuming that the target is located at position (x_0,y_0,z_0), and transmits at time τ_0. Assuming that there are N time synchronized sensors deployed at positions $(x_1,y_1,z_1),\ldots,(x_N,y_N,z_N)$, and that they receive the transmission from target mobile at times $\tau_1,\ldots,\tau_N$. For sensor $i\in 1\ldots N$, the following cost function may be derived:

$$f_{TDOA}^{i}(x)=\sqrt{(x_i-x)^2+(y_i-y)^2+(z_i-z)^2}-c(\tau_i-\tau), \tag{34}$$

where c is the speed of light, and $x=[x\ y\ z\ \tau]^T$ is the unknown vector which contains the current estimated position of the target and the estimated target transmission time. This function takes on a low value ideally (and in the absence of all error sources) at all sensors when $x=[x_0 y_0 y_0 \tau_0]^T$.

The cost function specific to the hyperbolic based synchronized TDOA is derived as follows:

$$f_{TDOA}^{i}(x)-f_{TDOA}^{i+1}(x)=\sqrt{(x_i-x)^2+(y_i-y)^2+(z_i-z)^2}-\sqrt{(x_{i+1}-x)^2+(y_{i+1}-y)^2+(z_{i+1}-z)^2}-c(\tau_i-\tau)+c(\tau_{i+1}-\tau) \tag{35}$$

$$f_{TDOA}^{i}(x)-f_{TDOA}^{i+1}(x)=\sqrt{(x_i-x)^2+(y_i-y)^2+(z_i-z)^2}-\sqrt{(x_{i+1}-x)^2+(y_{i+1}-y)^2+(z_{i+1}-z)^2}-c(\tau_i-\tau_{i+1}) \tag{36}$$

$$f_{HYP}^{\ i}(x)=f_{TDOA}^{\ i}(x)-f_{TDOA}^{\ i+1}(x),\ \text{where}\ x=(x_0,y_0,z_0)^T. \tag{37}$$

The cost function may be dependent only on the measured time difference of arrival between relevant sensors and the position of the target. Given a perfect measurement in ideal conditions, this cost function approaches zero as the estimate approaches the actual target location. The estimate vector in this case is free of the unknown target transmit time, as this has been subtracted out and is of no practical interest for the location estimation application. The remainder of the development for the hyperbolic case follows that presented in section 2 above.

The overall cost function is as described in equation (3), where $f_i(x)$ is replaced with $f_{HYP}^{\ i}(x)$. The relevant partial derivatives of $f_{HYP}^{\ i}(x)$ are determined as shown below. Let $u_i=(x_i-x)^2+(y_i-y)^2+(z_i-z)^2$, then rewrite the cost function in equation (37) as:

$$f_{HYP}^{\ i}(x)=\sqrt{u_i}^2-\sqrt{u_{i+1}}^2-c(\tau_i-\tau_{i+1}). \tag{38}$$

Now using differential Calculus, the partial derivative of the cost function in equation (38) is

$$\frac{\delta f_{HYP}^{i}(x)}{\delta x}=\frac{1}{2\sqrt{u_i}}\cdot\frac{\delta u_i}{\delta x}-\frac{1}{2\sqrt{u_{i+1}}}\cdot\frac{\delta u_{i+1}}{\delta x}=\frac{1}{2\sqrt{u_i}}\cdot 2(x_i-x)\cdot(-1)-\frac{1}{2\sqrt{u_{i+1}}}\cdot \tag{39}$$

-continued

$$= \frac{2(x_{i+1}-x)\cdot(-1)}{\sqrt{(x_i-x)^2+(y_i-y)^2+(z_i-z)^2}} - \frac{(x-x_i)}{\sqrt{(x_{i+1}-x)^2+(y_{i+1}-y)^2+(z_{i+1}-z)^2}},$$

so the final form of the partial derivatives of the system level cost function can be rewritten as:

$$\left.\frac{\delta F}{\delta x}\right|_{x_k} = 2\cdot\sum_{i=1}^{N}\alpha_i^2 f_{HYP}^i(x)\cdot\left\{\frac{(x_k-x_i)}{\sqrt{(x_i-x_k)^2+(y_i-y_k)^2+(z_i-z_k)^2}} - \frac{(x_k-x_{i+1})}{\sqrt{(x_{i+1}-x_k)^2+(y_{i+1}-y_k)^2+(z_{i+1}-z_k)^2}}\right\}. \quad (40)$$

In like fashion, the other partial derivatives functions can be derived and are summarized below.

$$\left.\frac{\delta F}{\delta y}\right|_{y_k} = 2\cdot\sum_{i=1}^{N}\alpha_i^2 f_{HYP}^i(x)\cdot\left\{\frac{(y_k-y_i)}{\sqrt{(x_i-x_k)^2+(y_i-y_k)^2+(z_i-z_k)^2}} - \frac{(y_k-y_{i+1})}{\sqrt{(x_{i+1}-x_k)^2+(y_{i+1}-y_k)^2+(z_{i+1}-z_k)^2}}\right\} \quad (41)$$

$$\left.\frac{\delta F}{\delta z}\right|_{z_k} = 2\cdot\sum_{i=1}^{N}\alpha_i^2 f_{HYP}^i(x)\cdot\left\{\frac{(z_k-z_i)}{\sqrt{(x_i-x_k)^2+(y_i-y_k)^2+(z_i-z_k)^2}} - \frac{(z_k-z_{i+1})}{\sqrt{(x_{i+1}-x_k)^2+(y_{i+1}-y_k)^2+(z_{i+1}-z_k)^2}}\right\} \quad (42)$$

Compare these equations to equations (9)-(11), respectively. In summary, the NLSSDA for the TDOA method is described by equations (4), (5), and (40)-(42).

Section 6: Data Fusion Across Measurement Families

The various measurements and equations derived in previous sections can be combined and used simultaneously in the same algorithm (i.e., data fusion). In this case, the adaptive algorithm combines the various measurements, and families of measurements, in a weighted least-squares sense. Assuming that there are N sensor measurements, there are N equations for methods that are not differential in nature (i.e., TOF and AOA methods), and M equations for methods that are differential in nature (i.e., relative RSSI method, and TDOA).

If imposing a restriction that utilizes only independent sensor combinations, then M=N−1. It has been established (via simulations) that with noise and all other error sources enabled, using all of the dependent combinations in addition to the independent combinations affords better performance as a result of averaging the noise and errors components. In the case where all combinations of sensors are used, M=1+2+ . . . +N−1, there are N_{RSSI}=M RSSI based equations, N_{HYP}=M TDOA based equations, N_{TOF}=N TOF based equations, and N_{ANG}=N AOA based equations. The equations discussed in the previous sections are combined to form the overall cost function as follows:

$$F_{COM}(x) = \sum_{i=1}^{N_{TOF}}\alpha_i^2 f_i^2(x) + \sum_{i=1}^{N_{RSSI}}\alpha_{RSSI,i}^2 f_{RSSI,i}^2(x) + \sum_{i=1}^{N_{ANG}}\alpha_{ANG,i}^2 f_{ANG,i}^2(x) + \sum_{i=1}^{N_{HYP}}\alpha_{HYP,i}^2 f_{HYP,i}^2(x) \quad (34)$$

The relevant partial derivatives of this function are easily determined using the property that the derivative of a sum of terms is the sum of the derivatives of the terms and using equations (9)-(11), (23)-(25), (31)-(33), and (40)-(42), which have been previously derived. As usual, the position estimate of the target is updated according to the following equation:

$$x_{k+1} = x_k - \mu\nabla_x F_{COM}(x_k), \quad (35)$$

where

$$\nabla_x F_{COM}(x_k) = \nabla_x F_{COM}(x)|_{x_k} = \begin{pmatrix} \left.\frac{\delta F_{COM}}{\delta x}\right|_{x_k} \\ \left.\frac{\delta F_{COM}}{\delta y}\right|_{y_k} \\ \left.\frac{\delta F_{COM}}{\delta z}\right|_{z_k} \end{pmatrix}.$$

Using this strategy, by judiciously choosing the α_i terms in (34), different families of measurements, indeed even measurements within families, can be combined in a weighted sense (including turning off by setting the relevant weights to 0) to arrive at a position estimate that is optimized in a weighted least-squares sense. In summary, the NLSSDA for this hybrid approach is described by equations (34), (35), and using the partial derivative terms in (9)-(11), (23)-(25), (31)-(33), and (40)-(42) in the computation of (35).

Section 7: Conclusion

Provided herein is the relevant mathematics used for full 3D geolocation using a variety of measurement families. In addition to providing a range of techniques for location estimation, this technique offers the ability to combine all of the various measurement families into a single algorithm so that a location estimate is computed which is optimum in a weighted least squared sense. The weighting is completely general. Individual measurements can be weighted relative to its peer's measurements, or entire measurement families can be weighted relative to other families of measurements.

Many modifications and other embodiments of the invention will come to the mind of one skilled in the art having the benefit of the teachings presented in the foregoing descriptions and the associated drawings. Therefore, it is understood that the invention is not to be limited to the specific embodiments disclosed, and that modifications and embodiments are intended to be included within the scope of the appended claims.

That which is claimed is:

1. A location determining system for a wireless cellular transmitter, the location determining system to be carried by a platform movable relative to the wireless cellular transmitter and comprising:

an antenna;

a receiver coupled to said antenna; and

a location determining processor coupled to said receiver

to collect, during movement relative to the wireless cellular transmitter, a series of range measurements, a corresponding series of received signal measurements, a corresponding series of received signal strength measurements, and

to estimate a location of the wireless cellular transmitter based upon the range measurements and the received signal strength measurements, both weighted using the received signal measurements.

2. The location determining system according to claim **1** further comprising a platform position determining device; and wherein said location determining processor cooperates with said platform position determining device so that the estimated location of the wireless cellular transmitter comprises an estimated geolocation.

3. The location determining system according to claim **1** wherein said location determining processor further estimates an elevation of the wireless cellular transmitter.

4. The location determining system according to claim **1** wherein the received signal measurements comprise at least one of bit-error rate measurements, receiver metrics, and signal-to-noise ratio measurements.

5. The location determining system according to claim **1** wherein said location determining processor estimates the location of the wireless cellular transmitter based upon a least-squares steepest decent algorithm.

6. The location determining system according to claim **1** wherein said location determining processor collects the series of range measurements using time of flight measurements.

7. The location determining system according to claim **1** wherein said antenna comprises a directional antenna; wherein said location determining processor cooperates with said directional antenna to collect, during movement relative to the wireless cellular transmitter, a corresponding series of angle of arrival measurements; and wherein said location determining processor estimates the location of the wireless cellular transmitter further based upon the angle of arrival measurements.

8. The location determining system according to claim **7** wherein said location determining processor weights the angle of arrival measurements based upon the received signal measurements.

9. The location determining system according to claim **1** wherein the platform comprises an aircraft.

10. The location determining system according to claim **1** wherein the platform comprises a ground-based vehicle.

11. A location determining system for a wireless cellular transmitter, the location determining system to be carried by a platform movable relative to the wireless cellular transmitter and comprising:

a directional antenna;

a receiver coupled to said directional antenna;

a platform position determining device; and

a location determining processor coupled to said receiver and said platform position determining device for

collecting, during movement relative to the wireless cellular transmitter, a series of range measurements, a corresponding series of received signal measurements, a corresponding series of angle of arrival measurements, and a corresponding series of received signal strength measurements, and

estimating a geolocation of the wireless cellular transmitter based upon the range measurements, the angle of arrival measurements, the received signal strength measurements, each weighted using the received signal measurements.

12. The location determining system according to claim **11** wherein the received signal measurements comprise at least one of bit-error rate measurements, receiver metrics, and signal-to-noise ratio measurements.

13. The location determining system according to claim **11** wherein said location determining processor estimates the location of the wireless cellular transmitter based upon a least-squares steepest decent algorithm.

14. The location determining system according to claim **11** wherein said location determining processor collects the series of range measurements using time of flight measurements.

15. A method of estimating a location of a wireless cellular transmitter using a location determining system, the method comprising:

collecting, during movement of the location determining system relative to the wireless cellular transmitter, a series of range measurements, a corresponding series of received signal measurements, and a corresponding series of received signal strength measurements; and

estimating a location of the wireless cellular transmitter based upon the range measurements and the received signal strength measurements, both weighted using the received signal measurements.

16. The method according to claim **15** further comprising collecting, during movement of the location determining system relative to the wireless cellular transmitter, a corresponding series of angle of arrival measurements; and wherein estimating the location of the wireless cellular transmitter comprises estimating the location further based upon the angle of arrival measurements.

17. The method according to claim **15** wherein estimating the location of the wireless cellular transmitter comprises estimating a geolocation of the wireless cellular transmitter.

18. The method according to claim **15** wherein estimating the location of the wireless cellular transmitter comprises estimating an elevation of the wireless cellular transmitter.

19. The method according to claim **15** wherein the received signal measurements comprise at least one of bit-error rate measurements, receiver metrics, and signal-to-noise ratio measurements.

20. The method according to claim **15** wherein estimating the location of the wireless cellular transmitter comprises estimating the location of the wireless cellular transmitter based upon a least-squares steepest decent algorithm.

21. The method according to claim **15** wherein collecting the series of range measurements comprises collecting a series of time of flight measurements.

* * * * *

EXHIBIT 32	Catherine Crump, ACLU FOIA request to USDOJ (November 29, 2007), *available at* <http://www.aclu.org/files/pdfs/freespeech/eousa_foia_20071129.pdf > (last accessed Mar. 30, 2011);
EXHIBIT 32	
EXHIBIT 32	
EXHIBIT 32

November 29, 2007

VIA FACSIMILE AND FEDERAL EXPRESS

FOIA/Privacy Staff
Executive Office for United States Attorneys
United States Department of Justice
Suite 7300, Bicentennial Building
600 E Street, N.W.
Washington, DC 20530-0001
Fax: 202.616.6478

Re: REQUEST UNDER FREEDOM OF INFORMATION ACT / Expedited Processing Requested

Attention:

This letter constitutes a request by the American Civil Liberties Union and the American Civil Liberties Union Foundation ("ACLU") under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552 *et seq.*, and the Department of Justice implementing regulations, 28 C.F.R. § 16.1 *et seq.*[1]

I. The Request for Information

Recent court decisions and media reports reveal that United States Attorneys Offices ("USAOs") are assisting law enforcement officers in obtaining information from mobile carriers that enables officers to track the location of individuals' mobile phones.[2] Court decisions indicate that USAOs claim not to need probable cause to obtain real-time tracking information. News reports further suggest that some field offices are violating a Department of Justice "internal recommendation" that "federal prosecutors seek warrants based on probable cause to obtain precise location data in

[1] The American Civil Liberties Union Foundation is a 501(c)(3) organization that provides legal representation free of charge to individuals and organizations in civil rights and civil liberties cases, and educates the public about civil rights and civil liberties issues. The American Civil Liberties Union is a separate non-profit, non-partisan, 501(c)(4) membership organization that educates the public about the civil liberties implications of pending and proposed state and federal legislation, provides analyses of pending and proposed legislation, directly lobbies legislators, and mobilizes its members to lobby their legislators.

[2] Ellen Nakashima, *Cellphone Tracking Powers on Request*, Washington Post, Page A01, Nov. 23, 2007, available at http://www.washingtonpost.com/wp-dyn/content/article/2007/11/22/AR2007112201444_2.html?hpid=topnews.

private areas."[3] Also, news reports raise the possibility that on at least some occasions, law enforcement officers obtain tracking data directly from mobile carriers without any court involvement whatsoever.[4]

This request seeks information regarding these practices. Accordingly, the ACLU seeks disclosure of records regarding:

1. Policies, procedures, and practices followed to obtain mobile phone location information for law enforcement purposes;

2. The "internal recommendation" that "federal prosecutors seek warrants based on probable cause to obtain precise location data in private areas" described in Ellen Nakashima, *Cellphone Tracking Powers on Request*, Washington Post, Page A01, Nov. 23, 2007, attached as Appendix A;

3. Any violations of the "internal recommendation";

4. The number of times the government has applied for a court order, based on less than probable cause, authorizing it to obtain mobile phone location information, and whether such applications were successful;

5. The case name, docket number, and court of all criminal prosecutions, current or past, of individuals who were tracked using mobile location data, where the government did not first secure a warrant based on probable cause for such data.

II. Offices to be Searched

We request that you search the following EOUSA Staffs: Office of the Director, Counsel to the Director, Attorney General Advisory Committee, Legal Programs, and General Counsel. In formulating this list, we relied on the staff descriptions available at www.usdoj.gov/usao/eousa/staff.html#lp.

In addition, we request that you search the United States Attorneys' Offices in the following locations: California, District of Columbia, Indiana, Louisiana, New Jersey, Florida, and Nevada. For each state listed above, please search all United States Attorneys' Offices within the state.

---

[3] *Id.*

[4] *Id.* ("Justice Department officials said to the best of their knowledge, agents are obtaining court approval unless the carriers provide the data voluntarily.")

III. Limitation of Processing Fees

The ACLU requests a limitation of processing fees pursuant to 5 U.S.C. § 552(a)(4)(A)(ii)(II) ("fees shall be limited to reasonable standard charges for document duplication when records are not sought for commercial use and the request is made by . . . a representative of the news media . . .") and 28 C.F.R. §§ 16.11(c)(1)(i), 16.11(d)(1) (search and review fees shall not be charged to "representatives of the news media."). As a "representative of the news media," the ACLU fits within this statutory and regulatory mandate. Fees associated with the processing of this request should, therefore, be limited accordingly.

The ACLU meets the definition of a "representative of the news media" because it is "an entity that gathers information of potential interest to a segment of the public, uses its editorial skills to turn raw materials into a distinct work, and distributes that work to an audience." *National Security Archive v. Department of Defense*, 880 F.2d 1381, 1387 (D.C. Cir. 1989).

The ACLU is a national organization dedicated to the defense of civil rights and civil liberties. Dissemination of information to the public is a critical and substantial component of the ACLU's mission and work. Specifically, the ACLU publishes newsletters, news briefings, right-to-know documents, and other educational and informational materials that are broadly disseminated to the public. Such material is widely available to everyone, including individuals, tax-exempt organizations, not-for-profit groups, law students and faculty, for no cost or for a nominal fee through its public education department. The ACLU also disseminates information through its heavily visited web site: http://www.aclu.org/. The web site addresses civil rights and civil liberties issues in depth, provides features on civil rights and civil liberties issues in the news, and contains many thousands of documents relating to the issues on which the ACLU is focused. The website specifically includes features on information obtained through the FOIA. *See, e.g.*, www.aclu.org/patriot_foia; www.aclu.org/torturefoia; http://www.aclu.org/spyfiles. The ACLU also publishes an electronic newsletter, which is distributed to subscribers by e-mail.

In addition to the national ACLU offices, there are 53 ACLU affiliate and national chapter offices located throughout the United States and Puerto Rico. These offices further disseminate ACLU material to local residents, schools and organizations through a variety of means including their own websites, publications and newsletters. Further, the ACLU makes archived

material available at the American Civil Liberties Union Archives, Public Policy Papers, Department of Rare Books and Special Collections, Princeton University Library. ACLU publications are often disseminated to relevant groups across the country, which then further distribute them to their members or to other parties.

Depending on the results of the Request, the ACLU plans to "disseminate the information" gathered by this Request "among the public" through these kinds of publications in these kinds of channels. The ACLU is therefore a "news media entity." *Cf. Electronic Privacy Information Ctr. v. Department of Defense*, 241 F. Supp. 2d 5, 10-15 (D.D.C. 2003) (finding non-profit public interest group that disseminated an electronic newsletter and published books was a "representative of the media" for purposes of FOIA).

Disclosure is not in the ACLU's commercial interest. The ACLU is a "non-profit, non-partisan, public interest organization." *See Judicial Watch Inc. v. Rossotti*, 326 F.3d 1309, 1310 (D.C. Cir. 2003). Any information disclosed by the ACLU as a result of this FOIA will be available to the public at no cost.

IV. Waiver of all Costs

The ACLU additionally requests a waiver of all costs pursuant to 5 U.S.C. § 552(a)(4)(A)(iii) ("Documents shall be furnished without any charge . . . if disclosure of the information is in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the government and is not primarily in the commercial interest of the requester."). Disclosure in this case meets the statutory criteria, and a fee waiver would fulfill Congress's legislative intent in amending FOIA. *See Judicial Watch, Inc. v. Rossotti*, 326 F.3d 1309, 1312 (D.C. Cir. 2003) ("Congress amended FOIA to ensure that it be 'liberally construed in favor of waivers for noncommercial requesters.'").

Disclosure of the requested information will help members of the public understand the privacy risks of carrying a mobile phone. The government's policies and practices for monitoring the locations of mobile phones are unclear. It is not even apparent whether the government routinely obtains mobile phone location information without any court supervision whatsoever. Under these circumstances, there is little doubt that the requested information will "contribute significantly to public understanding." 5 U.S.C. § 552(a)(4)(A)(iii).

As a nonprofit 501(c)(3) organization and "representative of the news media" as discussed in Section III, the ACLU is well-situated to disseminate information it gains from this request to the general public and to groups that protect constitutional rights. Because the ACLU meets the test for a fee waiver, fees associated with responding to FOIA requests are regularly waived for the ACLU.[5]

The records requested are not sought for commercial use, and the requesters plan to disseminate the information disclosed as a result of this FOIA request through the channels described in Section III. As also stated in Section III, the ACLU will make any information disclosed as a result of this FOIA available to the public at no cost.

V. Expedited Processing Request

Expedited processing is warranted because there is "[a]n urgency to inform the public about an actual or alleged federal government activity" by organizations "primarily engaged in disseminating information." 28 C.F.R. § 16.5(d)(1)(ii).[6]

The overwhelming majority of Americans—over 200 million people—carry mobile phones.[7] This large number is steadily increasing. The information the ACLU seeks therefore bears on the privacy of a vast segment of the United States population.

The limited information currently available about the government's tracking practices raises serious questions about whether the government is

---

[5] For example, in May 2005, the United States Department of Commerce granted a fee waiver to the ACLU with respect to its request for information regarding the radio frequency identification chips in United States passports. In March 2005, the Department of State granted a fee waiver to the ACLU with regard to a request submitted that month regarding the use of immigration laws to exclude prominent non-citizen scholars and intellectuals from the country because of their political views, statements, or associations. Also, the Department of Health and Human Services granted a fee waiver to the ACLU with regard to a FOIA request submitted in August of 2004. In addition, the Office of Science and Technology Policy in the Executive Office of the President said it would waive the fees associated with a FOIA request submitted by the ACLU in August 2003. In addition, three separate agencies – the Federal Bureau of Investigation, the Office of Intelligence Policy and Review, and the Office of Information and Privacy in the Department of Justice – did not charge the ACLU fees associated with a FOIA request submitted by the ACLU in August 2002.

[6] The ACLU is "primarily engaged in disseminating information," as discussed in Sections III and IV.

[7] CTIA—The Wireless Association—Survey Results, June 2007, available at http://www.ctia.org/media/press/body.cfm/prid/1717.

complying with the law and the Constitution. The courts are divided on whether it is lawful for the government to track individuals without first obtaining a warrant based on probable cause. Several judges have held that the government lacks this authority.[8] It now seems likely that the government's view of its surveillance powers is even more expansive than previously thought, and that it believes it can access such information without any court oversight whatsoever.

Given the pervasive nature of cell phone ownership, and the lack of clarity regarding the privacy individuals using cell phones can expect, there is "[a]n urgency to inform the public about an actual or alleged federal government activity." 28 C.F.R. § 16.5(d)(1)(ii).

This FOIA request is entitled to expedited processing for a second reason. The information sought relates to "a matter of widespread and exceptional media interest in which there exist possible questions about the government's integrity which affect public confidence." 28 C.F.R. § 16.5(d)(1)(iv).

The dubious legality of the government's actions, described above, raise questions about the government's integrity. Further, there is exceptional media interest in the government's tracking of mobile phones. The most recent rash of news coverage was prompted by the Washington Post story discussed above.[9] Newspapers across the country deemed the Washington Post article sufficiently important that it was reprinted in the Charlotte Observer, Chicago Tribune, Cincinnati Post, Houston Chronicle, Lexington Herald-Leader, Pittsburgh Post-Gazette, Seattle Times, South Florida Sun-Sentinel, and St. Paul Pioneer Press. Other publications ran their own stories on the subject.[10] National television stations immediately devoted coverage to

---

[8] *See, e.g.*, In the Matter of the Application of the UNITED STATES of America for ORDERS AUTHORIZING the INSTALLATION and Use of PEN REGISTERS and Caller Identification Devices on Telephone Numbers [Sealed] and [Sealed], 416 F.Supp.2d 390, 391 (D. Md. 2006) ("Unless and until Congress takes further action, the court may only authorize disclosure of prospective cell site information upon a showing of probable cause pursuant to Rule 41."); In the Matter of an APPLICATION OF THE UNITED STATES FOR AN ORDER (1) AUTHORIZING THE USE OF A PEN REGISTER AND A TRAP AND TRACE DEVICE and (2) Authorizing Release of Subscriber Information and/or Cell Site Information, 396 F.Supp.2d 294, 295 (E.D.N.Y. 2005) ("[E]xisting law does not permit the government to obtain the requested information on a prospective, real-time basis without a showing of probable cause.").

[9] Ellen Nakashima, *Cellphone Tracking Powers on Request*, Washington Post, Page A01, Nov. 23, 2007, Appendix A.

[10] *Justice Department Defends Use of Cell-Phone Tracking Data*, Fox News, Nov. 24, 2007, at http://www.foxnews.com/story/0,2933,312647,00.html; *Feds Push for Real-Time Cell-*

the story.[11] The revelations in the Washington Post story prompted editorial boards around the country to voice concern over Justice Department practices.[12] This recent coverage is only the most current example of persistent press interest in the government's use of cell phones as tracking devices.[13] Of course, the more general issue of the government's expansive view of its surveillance powers has been the subject of sustained news coverage, extensive congressional oversight hearings, and numerous lawsuits throughout the country.

The ACLU expects the determination of this request for expedited processing within 10 calendar days and the determination of this request for documents within 20 days. *See* 28 CFR § 16.5(d)(4); 5 U.S.C. § 552(a)(6)(A)(i). If this request is denied in whole or in part, we ask that you justify all deletions by reference to specific exemptions to FOIA. We request the release of all segregable portions of otherwise exempt material. The

---

Phone Tracking Data, San Jose Mercury News, Nov. 23, 2007, at 4a; *Phone Tech Raises Privacy Concerns*, United Press International, Nov. 23, 2007.

[11] Cable News Network, Kelli Arena interviews Mark Rotenberg, Nov. 23, 2007, transcript available at 2007 WLNR 23221490; Fox News coverage, Nov. 23, 2007, transcript available at 2007 WLNR 23256527.

[12] Editorial, *Probable Abuse*, Albany Times Union, Nov. 27, 2007; Editorial, *Privacy Threat, Congress and the Judiciary Should Promulgate Tighter Rules for Government Access to Cell Phone Data*, Houston Chronicle, Nov. 25, 2007; Editorial, *Tracking You Down*, Syracuse Post-Standard, Nov. 25, 2007.

[13] Brendan I. Koerner, *Your Cellphone is a Homing Device*, Legal Affairs, July/August 2003; William B. Baker, *New York Case Tests Law of Surveillance on Cell Phone Location Data*, Privacy in Focus, Sept. 2005; Declan McCullagh, *Police Blotter: Cell Phone Tracking Rejected*, CNET News.com, Sept. 2, 2005, at: http://www.news.com/Police-blotter-Cell-phone-tracking-rejected/2100-1030_3-5846037.html; Al Gidari, *Yet Another Court Rules that Disclosure of Cell Site/Location Information Requires Probable Cause Showing*, Digestible Law: Perkins Coie's Internet Case Digest, Oct. 21, 2005; Ryan Singel, *U.S. Cell-Phone Tracking Clipped*, Wired, Oct. 27, 2005; Anita Ramasastry, *Every Move You Make, Part Three: Why Law Enforcement Should Have to Get a Warrant Before Tracking Us Via our Cell Phones*, FindLaw.com, Nov. 10, 2005, at: http://writ.news.findlaw.com/ramasastry/20051110.html; Matt Richtel, *Live Tracking of Mobile Phones Prompts Court Fights on Privacy*, New York Times, Dec. 10, 2005, at A1; Neal Conan, *NPR Talk of the Nation: Surveillance Via Cell Phone*, National Public Radio, Dec. 14, 2005; Tresa Baldas, *Feds' Cell Phone Tracking Divides the Courts*, The National Law Journal, Jan. 19, 2006; Scott Cameron, *Your Cell Phone Is A Homing Beacon – Should The Government Be Allowed To Use It Without Showing Probable Cause?*, The IP Law Blog, April 12, 2006; Stephen V. Treglia, *Trailing Cell Phones: Courts Grapple With Requests from Prosecutors Seeking Prospective Tracking*, New York Law Journal, July 18, 2006; Daniel R. Sovocool & Kristin Jamberdino, *Tracking a User's Location Via Cell Phone*, ipFrontline.com, Nov. 16, 2006, at: http://www.ipfrontline.com/depts/article.asp?id=9633&deptid=5; Linda Coady, *Government May Track Cell Phone Movements, N.Y. Court Says*, Privacy Litigation Reporter, Vol. 4:3, Nov. 17, 2006.

ACLU reserves the right to appeal a decision to withhold any information or to deny a waiver of fees.

Thank you for your prompt attention to this matter. Please furnish all applicable records to:

Catherine Crump
Staff Attorney
American Civil Liberties Union Foundation
125 Broad Street, 17th floor
New York, NY 10004

I affirm that the information provided supporting the request for expedited processing is true and correct to the best of my knowledge and belief.

Sincerely,

Catherine Crump
Staff Attorney
American Civil Liberties Union

Appendix

washingtonpost.com

Cellphone Tracking Powers on Request

Secret Warrants Granted Without Probable Cause

By Ellen Nakashima
Washington Post Staff Writer
Friday, November 23, 2007; A01

Federal officials are routinely asking courts to order cellphone companies to furnish real-time tracking data so they can pinpoint the whereabouts of drug traffickers, fugitives and other criminal suspects, according to judges and industry lawyers.

In some cases, judges have granted the requests without requiring the government to demonstrate that there is probable cause to believe that a crime is taking place or that the inquiry will yield evidence of a crime. Privacy advocates fear such a practice may expose average Americans to a new level of government scrutiny of their daily lives.

Such requests run counter to the Justice Department's internal recommendation that federal prosecutors seek warrants based on probable cause to obtain precise location data in private areas. The requests and orders are sealed at the government's request, so it is difficult to know how often the orders are issued or denied.

The issue is taking on greater relevance as wireless carriers are racing to offer sleek services that allow cellphone users to know with the touch of a button where their friends or families are. The companies are hoping to recoup investments they have made to meet a federal mandate to provide enhanced 911 (E911) location tracking. Sprint Nextel, for instance, boasts that its "loopt" service even sends an alert when a friend is near, "putting an end to missed connections in the mall, at the movies or around town."

With Verizon's Chaperone service, parents can set up a "geofence" around, say, a few city blocks and receive an automatic text message if their child, holding the cellphone, travels outside that area.

"Most people don't realize it, but they're carrying a tracking device in their pocket," said Kevin Bankston of the privacy advocacy group Electronic Frontier Foundation. "Cellphones can reveal very precise information about your location, and yet legal protections are very much up in the air."

In a stinging opinion this month, a federal judge in Texas denied a request by a Drug Enforcement Administration agent for data that would identify a drug trafficker's phone location by using the carrier's E911 tracking capability. E911 tracking systems read signals sent to satellites from a phone's Global Positioning System (GPS) chip or triangulated radio signals sent from phones to cell towers. Magistrate Judge Brian L. Owsley, of the Corpus Christi division of the Southern District of Texas, said the agent's affidavit failed to focus on "specifics necessary to establish probable cause, such as relevant dates, names and places."

Owsley decided to publish his opinion, which explained that the agent failed to provide "sufficient specific information to support the assertion" that the phone was being used in "criminal" activity. Instead, Owsley wrote, the agent simply alleged that the subject trafficked in narcotics and used the phone to do so. The agent stated that the DEA had " 'identified' or 'determined' certain matters," Owsley wrote, but "these identifications, determinations or revelations are not facts, but simply

conclusions by the agency."

Instead of seeking warrants based on probable cause, some federal prosecutors are applying for orders based on a standard lower than probable cause derived from two statutes: the Stored Communications Act and the Pen Register Statute, according to judges and industry lawyers. The orders are typically issued by magistrate judges in U.S. district courts, who often handle applications for search warrants.

In one case last month in a southwestern state, an FBI agent obtained precise location data with a court order based on the lower standard, citing "specific and articulable facts" showing reasonable grounds to believe the data are "relevant to an ongoing criminal investigation," said Al Gidari, a partner at Perkins Coie in Seattle, who reviews data requests for carriers.

Another magistrate judge, who has denied about a dozen such requests in the past six months, said some agents attach affidavits to their applications that merely assert that the evidence offered is "consistent with the probable cause standard" of Rule 41 of the Federal Rules of Criminal Procedure. The judge spoke on condition of anonymity because of the sensitivity of the issue.

"Law enforcement routinely now requests carriers to continuously 'ping' wireless devices of suspects to locate them when a call is not being made . . . so law enforcement can triangulate the precise location of a device and [seek] the location of all associates communicating with a target," wrote Christopher Guttman-McCabe, vice president of regulatory affairs for CTIA -- the Wireless Association, in a July comment to the Federal Communications Commission. He said the "lack of a consistent legal standard for tracking a user's location has made it difficult for carriers to comply" with law enforcement agencies' demands.

Gidari, who also represents CTIA, said he has never seen such a request that was based on probable cause.

Justice Department spokesman Dean Boyd said field attorneys should follow the department's policy. "We strongly recommend that prosecutors in the field obtain a warrant based on probable cause" to get location data "in a private area not accessible to the public," he said. "When we become aware of situations where this has not occurred, we contact the field office and discuss the matter."

The phone data can home in on a target to within about 30 feet, experts said.

Federal agents used exact real-time data in October 2006 to track a serial killer in Florida who was linked to at least six murders in four states, including that of a University of Virginia graduate student, whose body was found along the Blue Ridge Parkway. The killer died in a police shooting in Florida as he was attempting to flee.

"Law enforcement has absolutely no interest in tracking the locations of law-abiding citizens. None whatsoever," Boyd said. "What we're doing is going through the courts to lawfully obtain data that will help us locate criminal targets, sometimes in cases where lives are literally hanging in the balance, such as a child abduction or serial murderer on the loose."

In many cases, orders are being issued for cell-tower site data, which are less precise than the data derived from E911 signals. While the E911 technology could possibly tell officers what building a suspect was in, cell-tower site data give an area that could range from about three to 300 square miles.

Since 2005, federal magistrate judges in at least 17 cases have denied federal requests for the

less-precise cellphone tracking data absent a demonstration of probable cause that a crime is being committed. Some went out of their way to issue published opinions in these otherwise sealed cases.

"Permitting surreptitious conversion of a cellphone into a tracking device without probable cause raises serious Fourth Amendment concerns especially when the phone is in a house or other place where privacy is reasonably expected," said Judge Stephen William Smith of the Southern District of Texas, whose 2005 opinion on the matter was among the first published.

But judges in a majority of districts have ruled otherwise on this issue, Boyd said. Shortly after Smith issued his decision, a magistrate judge in the same district approved a federal request for cell-tower data without requiring probable cause. And in December 2005, Magistrate Judge Gabriel W. Gorenstein of the Southern District of New York, approving a request for cell-site data, wrote that because the government did not install the "tracking device" and the user chose to carry the phone and permit transmission of its information to a carrier, no warrant was needed.

These judges are issuing orders based on the lower standard, requiring a showing of "specific and articulable facts" showing reasonable grounds to believe the data will be "relevant and material" to a criminal investigation.

Boyd said the government believes this standard is sufficient for cell-site data. "This type of location information, which even in the best case only narrows a suspect's location to an area of several city blocks, is routinely generated, used and retained by wireless carriers in the normal course of business," he said.

The trend's secrecy is troubling, privacy advocates said. No government body tracks the number of cellphone location orders sought or obtained. Congressional oversight in this area is lacking, they said. And precise location data will be easier to get if the Federal Communication Commission adopts a Justice Department proposal to make the most detailed GPS data available automatically.

Often, Gidari said, federal agents tell a carrier they need real-time tracking data in an emergency but fail to follow up with the required court approval. Justice Department officials said to the best of their knowledge, agents are obtaining court approval unless the carriersprovide the data voluntarily.

To guard against abuse, Congress should require comprehensive reporting to the court and to Congress about how and how often the emergency authority is used, said John Morris, senior counsel for the Center for Democracy and Technology.

Staff researcher Richard Drezen contributed to this report.

View all comments that have been posted about this article.

Post a Comment

View all comments that have been posted about this article.

ATTACHED EXHIBITS
RESPONSE TO GOVERNMENT'S MEMORANDUM REGARDING LAW ENFORCEMENT PRIVILEGE AND REQUEST FOR AN EX PARTE AND IN CAMERA HEARING IF NECESSARY
CR08-814-PHX-DGC

↓ **EXHIBIT 33** ↓
↓ **EXHIBIT 33** ↓
↓ **EXHIBIT 33** ↓
↓ **EXHIBIT 33** ↓
↓ **EXHIBIT 33** ↓
↓ **EXHIBIT 33** ↓
↓ **EXHIBIT 33** ↓
↓ **EXHIBIT 33** ↓
↓ **EXHIBIT 33** ↓
↓ **EXHIBIT 33** ↓
↓ **EXHIBIT 33** ↓
↓ **EXHIBIT 33** ↓
↓ **EXHIBIT 33** ↓
↓ **EXHIBIT 33** ↓
↓ **EXHIBIT 33** ↓
↓ **EXHIBIT 33** ↓
↓ **EXHIBIT 33** ↓
↓ **EXHIBIT 33** ↓
↓ **EXHIBIT 33** ↓
↓ **EXHIBIT 33** ↓
↓ **EXHIBIT 33** ↓
↓ **EXHIBIT 33** ↓
↓ **EXHIBIT 33** ↓
↓ **EXHIBIT 33** ↓
↓ **EXHIBIT 33** ↓
↓ **EXHIBIT 33** ↓
↓ **EXHIBIT 33** ↓
↓ **EXHIBIT 33** ↓
↓ **EXHIBIT 33** ↓
↓ **EXHIBIT 33** ↓
↓ **EXHIBIT 33** ↓
↓ **EXHIBIT 33** ↓

USDOJ (M.D. La.) Response to ACLU FOIA Request No. 07-4130 (Aug. 12, 2008), *available at* <http://www.aclu.org/pdfs/freespeech/cellfoia_release_074130_20080812.pdf> (last accessed Jan. 11, 2011); (only relevant sections are included in this exhibit);

U.S. Department of Justice

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

Requester: Catherine Crump Request Number: 07-4130

Subject of Request: Mobile Phone Tracking (Item 1-4) AUG 12 2008

Dear Requester:

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

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

Enclosed please find:

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

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

Section 552

[ ] (b)(1)	[ ] (b)(4)	[ ] (b)(7)(B)	[**X**] (j)(2)
[ ] (b)(2)	[**X**] (b)(5)	[ ] (b)(7)(C)	[ ] (k)(2)
[ ] (b)(3)	[ ] (b)(6)	[ ] (b)(7)(D)	[ ] (k)(5)
_____	[ ] (b)(7)(A)	[**X**] (b)(7)(E)	[ ] _____
_____		[ ] (b)(7)(F)	

Section 552a

[X] 47 additional page(s) originated with another government component. **These records were found in the U.S. Attorney's Office files and may or may not be responsive to your request.** These records will be referred to the following component for review and direct response to you: Department of Justice, Criminal Division.

[X] 4 additional page(s) originated with another government component. **These records were found in the U.S. Attorney's Office files and may or may not be responsive to your request.** These records will be referred to the following component for consultation and our office will respond to you after their review: U.S. Marshals Service .

[X] See additional information attached.

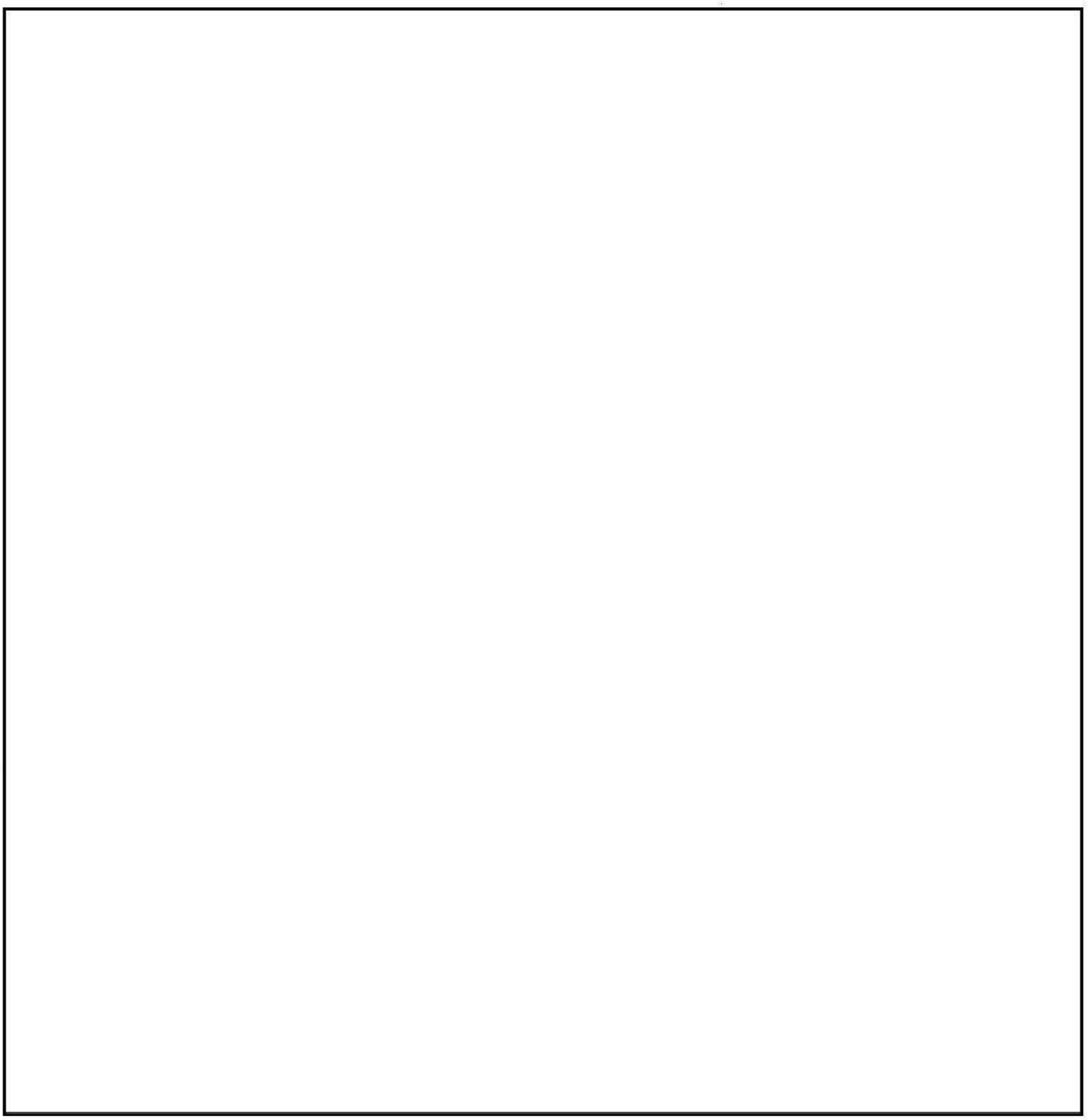
Although I am aware that this request is the subject of ongoing litigation and that appeals are not ordinarily acted on in such situations, I am required by statute and regulation to inform you that if you consider my response to be a denial of your request, you have the right to file an administrative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

Sincerely,

Karen M. Finnegan for

William G. Stewart II
Assistant Director

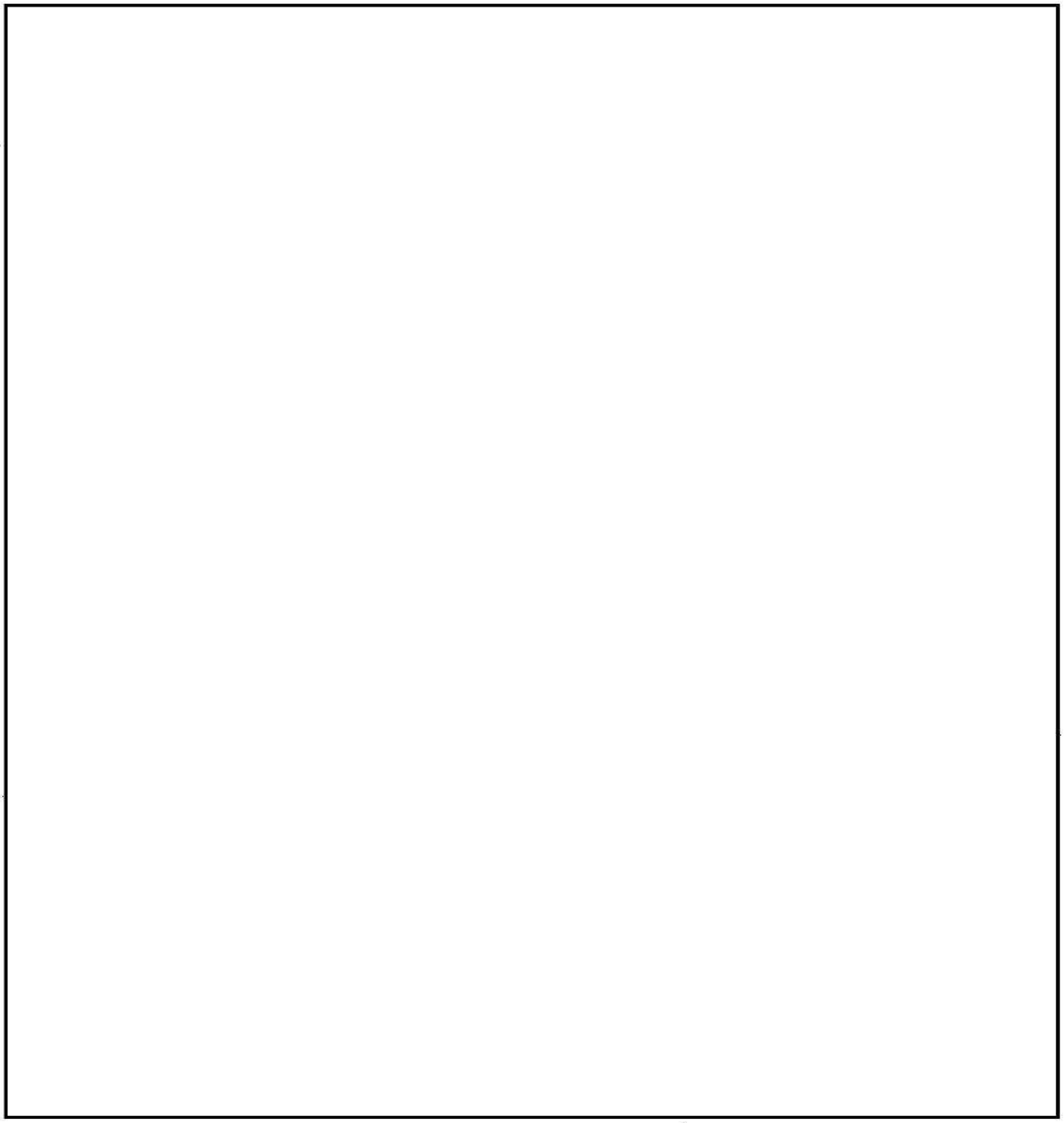
Enclosure(s)



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

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

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



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

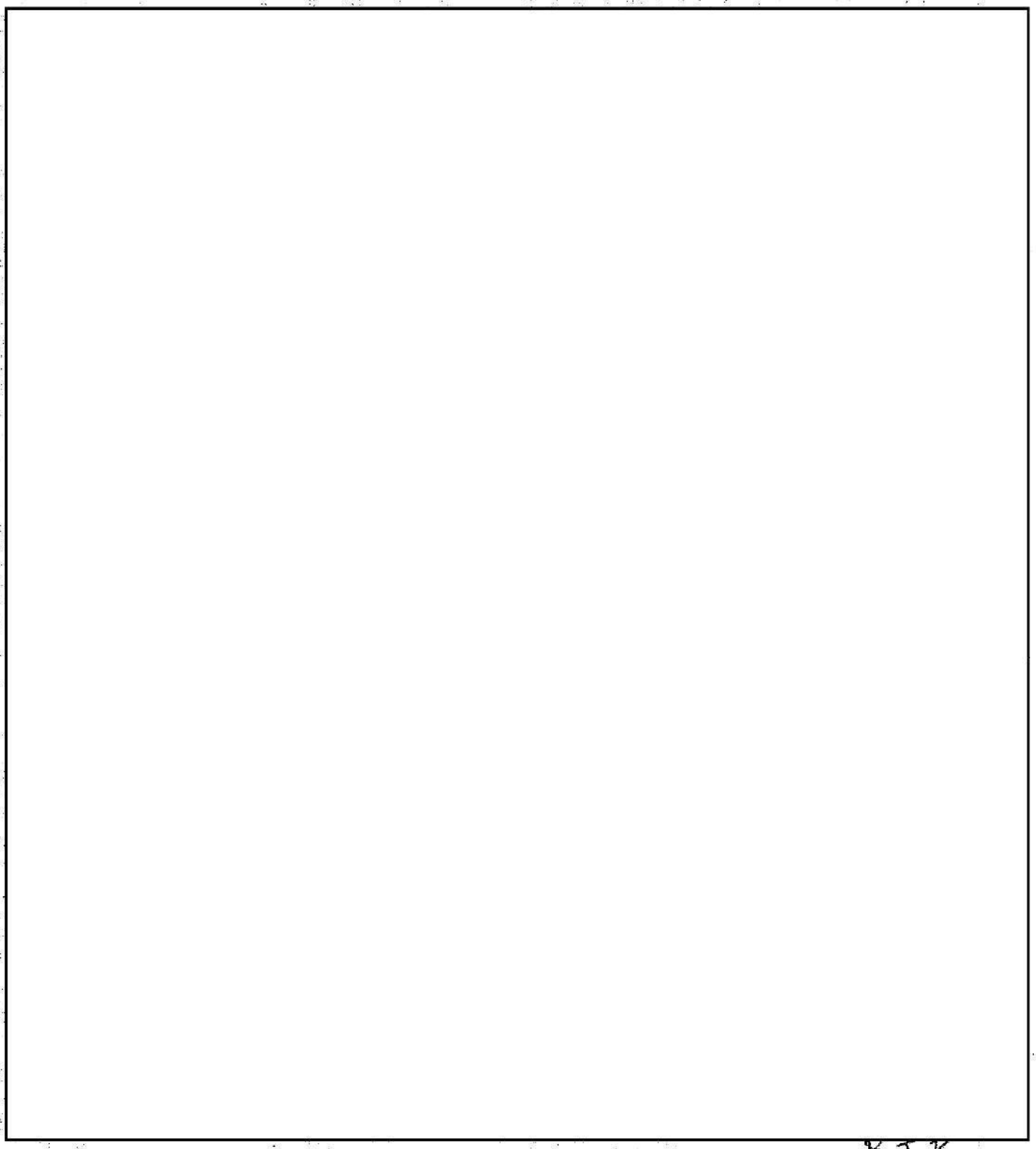
Practice note. See pen register forms (305-308) on USABook at **http://10.173.2.12/usao/eousa/ole/usabook/drug/forms**.

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.

USABook > Criminal Procedure > Electronic Surveillance > Pen Registers, Trap and Trace

- A **pen register**, also called a dialed number recorder (DNR), is a device that records the numbers dialed from a residential, business, or cellular telephone. A **trap and trace** is the reverse; it provides the telephone number calling a particular telephone.



RIP

EXHIBIT 34

FBI Response to EFF FOIA Request Nos. 1056287-000 & 1056307-1 (Aug. 27, 2007), *available at* <http://www.eff.org/files/filenode/061708CKK/082707_dcs01.pdf> (EFF PDF Set 1 of 6) (last accessed Jan. 11, 2011); (only relevant sections are included in this exhibit);

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D.C. 20535

ESQ. MARCIA HOFMANN
ELECTRONIC FRONTIER FOUNDATION
SUITE 650
1875 CONNECTICUT AVENUE, NORTHWEST
WASHINGTON, DC 20009

August 27, 2007

Subject: SYSTEM DCS-3000 and Red Hook

FOIPA No. 1056287- 000 and FOIPA No. 1056307-1

Dear Ms. Hofmann:

The enclosed documents were reviewed under the Freedom of Information/Privacy Acts (FOIPA), Title 5, United States Code, Section 552/552a. Deletions have been made to protect information which is exempt from disclosure, with the appropriate exemptions noted on the page next to the excision. In addition, a deleted page information sheet was inserted in the file to indicate where pages were withheld entirely. The exemptions used to withhold information are marked below and explained on the enclosed Form OPCA-16a:

Section 552		Section 552a
☒(b)(1)	☐(b)(7)(A)	☐(d)(5)
☒(b)(2)	☐(b)(7)(B)	☐(j)(2)
☐(b)(3)_____	☒(b)(7)(C)	☐(k)(1)
_____	☐(b)(7)(D)	☐(k)(2)
_____	☒(b)(7)(E)	☐(k)(3)
_____	☐(b)(7)(F)	☐(k)(4)
☐(b)(4)	☐(b)(8)	☐(k)(5)
☐(b)(5)	☐(b)(9)	☐(k)(6)
☒(b)(6)		☐(k)(7)

967 **page(s)** were reviewed and 618 **page(s)** are being released.

☐ Document(s) were located which originated with, or contained information concerning other Government agency(ies) [OGA]. This information has been:

- ☐ referred to the OGA for review and direct response to you.
- ☐ referred to the OGA for consultation. The FBI will correspond with you regarding this information when the consultation is finished.

☒ You have the right to appeal any denials in this release. Appeals should be directed in writing to the Director, Office of Information and Privacy, U.S. Department of Justice,1425 New York Ave., NW, Suite 11050, Washington, D.C. 20530-0001 within sixty days from the date of this letter. The envelope and the letter should be clearly marked "Freedom of Information Appeal" or "Information Appeal." Please cite the FOIPA number assigned to your request so that it may be easily identified.

☐ The enclosed material is from the main investigative file(s) in which the subject(s) of your request was the focus of the investigation. Our search located additional references, in files relating to other individuals, or matters, which may or may not be about your subject(s). Our experience has shown, when ident, references usually contain information similar to the information processed in the main file(s). Because of our significant backlog, we have given priority to processing only the main investigative file(s). If you want the references, you must submit a separate request for them in writing, and they will be reviewed at a later date, as time and resources permit.

☒ See additional information which follows.

Sincerely yours,

David M. Hardy
Section Chief
Record/Information
Dissemination Section
Records Management Division

Enclosure(s)

Please be advised that this is the fourth interim release as ordered by the court on May 7, 2007 for documents concerning surveillance systems known as DCS-3000 and Red Hook.

A decision has not been made concerning your request for a waiver of fees. We will be corresponding with you concerning that request in the near future. In the interim, we are providing you with the enclosed documents. Pursuant to Title 28, Code of Federal Regulations, Section 16.11, there is a fee of ten cents per page for duplication. No fees are assessed for the first 100 pages. If it is determined that you do not qualify for a fee waiver, duplication fees will be assessed accordingly.

[redacted] (OTD) (FBI)

From: [redacted] (OTD) (FBI)
Sent: Monday, May 22, 2006 8:56 AM
To: [redacted] CID) (FBI)
Subject: RE: Fd 71

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]

another area of technology you and your crew should be looking into are the [redacted]..while this is not the same as the hardware you have been procuring, there will more than likely be incidents in which you could leverage their capabilities. if memory serves me correct, there are only a few major manufacturers out there. as you will see listed in the [redacted] I sent you, while a user can disable the [redacted] of a handset - they *cannot* disable the [redacted] Now I haven't had the opportunity to do a lot of research into the standard [redacted] but I bet there is a wealth of information in there that could be of great benefit (in the past I used to research the standards to help identify and develop a lot of the capabilities your guys are currently using). Acquiring this documentation, along with establishing one-on-one relationships with the hardware manufacturers (and the appropriate personnel at the service provider) will guarantee success and a robust program as there are usually 'undocumented' capabilities that you can access to provide you with the information you need to locate handsets - these are the capabilities that you can bet that the guys in OTD (ATU/WITT, TICTU, etc.) will not share with you...thanks! mQ>

b2
b7E

-----Original Message-----
From: [redacted] CID) (FBI)
Sent: Friday, May 19, 2006 3:21 PM
To: [redacted] (OTD) (FBI)
Subject: RE: Fd 71

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

THANK YOU SIR. RJ

-----Original Message-----
From: [redacted] (OTD) (FBI)
Sent: Friday, May 19, 2006 3:16 PM
To: [redacted] (CID) (FBI)
Subject: RE: Fd 71

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]

this sounds as though it is the *correct* 3W amp...however, some of those amps had a power connector that appears to be very similar to an [redacted] connector. In the past, these types of connectors routinely failed - that is they failed to provide consistent contact with the power connector that is mounted to the amp. if your guy is dealing with this type of connector, I would strongly suggest that he attempt to verify power connectivity - preferably by monitoring the amount of current the amp is drawing during transmit (connecting it to a DC plug that has a current gauge, or, by inserting a current meter in series with either the

b2
b7E

power or ground wire). past experience shows that even when the amp felt 'warm' to the touch it was not operating consistently, but rather intermittently - hence the sometimes work other time not work experience....i'm not saying that this is the problem, only that it's a good place to start looking.

also, not meaning to sound condescending but, sometimes in the 'heat of battle' cables are connected improperly - that is, the IN gets connected to the OUT and vise versa...always verify that the hardware is properly installed whenever you feel things aren't working properly. One last thing to validate is whether or not the AMP was enabled on the software...

b2
b7E

What kinds of antennae are your guys using? covert? hi-gain?

There are a couple of additional items (more technical in nature) but we'll wait to see if its one of these before we get into them...also, when we have more time I'll go over the 3W vs. 10W debate....more W doesn't always mean better performance.

let me know...thanks!
mQ>

b6
b7C

-----Original Message-----
From: [redacted]CID) (FBI)
Sent: Friday, May 19, 2006 2:42 PM
To: [redacted](OTD) (FBI)
Subject: FW: Fd 71

UNCLASSIFIED
NON-RECORD

[redacted] FYI from Phoenix. rj

b6
b7C

-----Original Message-----
From: [redacted](PX) (FBI)
Sent: Friday, May 19, 2006 2:39 PM
To: [redacted](CID) (FBI); [redacted](KX) (FBI); [redacted]CG) (FBI); [redacted]MM) (FBI); [redacted]DN) (FBI); [redacted](LA) (FBI); [redacted](LA) (FBI); [redacted](LV) (FBI); [redacted](PH) (FBI); [redacted]DE) (FBI); [redacted](MP) (FBI); [redacted](SE) (FBI); [redacted](PH) (FBI)
Subject: RE: Fd 71

UNCLASSIFIED
NON-RECORD

[redacted]

The amp came with a quick reference guide that shows how the amp should be hooked up to a [redacted]. On the reverse side of the guide it shows [redacted] connections". The amp base plate is 10-12 inches long and three inches wide. It has an [redacted]n connection on one end and an [redacted]out connection on the opposite end. Is also has a plug for 12VDC in on the same end as the [redacted]n connection. There are two large screws on either end of the base plate that allow it to be screwed into the [redacted] There are twelve thin black rectangular pieces sticking straight up from the amp which is centered on the base plate. The rectangles are approximately two inches high and three inches long. There is NO fan for the amp. The amp is of the same design as the 3 wat amp that we had in Chantilly prior to being given a 10 watt amp.

b2
b7E

If need be, I can fax a copy of the quick reference guide to whoever would like to see it...

[redacted]

b6
b7C

-----Original Message-----
From: [redacted]CID) (FBI)
Sent: Friday, May 19, 2006 10:58 AM
To: [redacted]KX) (FBI); [redacted](CG) (FBI); [redacted]MM) (FBI); [redacted]DN) (FBI); [redacted](LA) (FBI); [redacted](LA) (FBI); [redacted](LV) (FBI);

[redacted] PX) (FBI) [redacted] (PH) (FBI); [redacted] DE) (FBI);
[redacted] (MP) (FBI) [redacted] SE) (FBI); [redacted] (PH) (FBI)

Subject: FW: Fd 71
Importance: High

UNCLASSIFIED
NON-RECORD

b6
b7C

Okay men (specifically [redacted] here's some tech talk in response to [redacted] tracking mission. Send your reply to me and I'll forward for a response. Thanks, [redacted]

UNCLASSIFIED
NON-RECORD

[redacted] your guy mentioned [redacted] .I am assuming that wasn't the system they were using. If the amp was originally meant for a [redacted] I am curious as to what amp it is. are there markings on the amp? can someone provide a description of it? or a digital picture? the reason I'm asking is that there are a lot of *old* three watt amps out there that were deployed with legacy (primarily analog) systems that sometimes make there way back into the new equipment line....if its one of those *old* amps, that amp is made for 800Mhz and will not amplify a PCS band signal (it will probably attenuate it instead)...also, were they operating in [redacted] modes? [redacted]

b2
b7E

UNCLASSIFIED
NON-RECORD

FYI. rj

-----Original Message-----
From: [redacted] (PX) (FBI)
Sent: Thursday, May 18, 2006 1:38 PM
To: [redacted] CID) (FBI)
Subject: RE: Fd 71

b6
b7C

UNCLASSIFIED
NON-RECORD

I've sent [redacted] an e-mail or two about it and advised of our ability to [redacted] but he has not responded...

On another note, Got a call from Memphis yesterday, sent them Philly's pen and trap order docs and then last night at 8:30p we went up on three phones (no thanks to the Memphis TTA's who never got the DCS3000 up and running) using [redacted] data and were able to immediately lock on one of the target phones at location one, and found a Van w/ TN plates at location 2, which promptly drove to location 1 and we got a hit on a second phone. At that point we just jumped the guys and took them into custody yada yada yada. The only problem we had with the gear [redacted] side of the house) was the same problem we had in Chantilly, although we could pick up the phone in collection mode, we could not get it to lock on with the [redacted] to pinpoint a direction. It may have something to do with the fact that we were only sent a 3 watt amp (for the [redacted] (sp)) instead of the 10 watt amp.

b2
b7E

Anyway, another success story for the MEN OF VCMO!!! I have a bunch of evidence and 302s/Ecs to draw up as well as prisoner transport and court, so I will get the WITT sheet done tomorrow...

b6
b7C

Later

[redacted]

[redacted](OTD) (FBI)

b6
b7C

From: [redacted]WF) (FBI)
Sent: Thursday, September 16, 2004 10:12 AM
To: [redacted](RH) (FBI);[redacted](BA) (FBI);[redacted] [redacted](WF) (FBI);[redacted](CE) (FBI);[redacted]RH) (FBI);[redacted]RH) (FBI);[redacted](BA) (FBI);[redacted](NE) (FBI)[redacted] [redacted](WF) (FBI);[redacted](WF) (FBI);[redacted](WF) (FBI);[redacted](WF) (FBI);[redacted](WF) (FBI);[redacted] [redacted](WF) (FBI);[redacted](WF) (FBI);[redacted](WF) (FBI);[redacted] [redacted](WF) (FBI)[redacted](WF) (FBI);[redacted](WF) (FBI);[redacted](WF) (FBI);[redacted]WF) (FBI);[redacted] (WF) (FBI);[redacted]WF) (FBI);[redacted](WF) (FBI);[redacted] [redacted](WF) (FBI);[redacted](WF) (FBI)
Cc: [redacted](ITD) (FBI);[redacted](ITD) (FBI);[redacted](ITD) (FBI);[redacted](ITD) (FBI);[redacted]ITD) (FBI)
Subject: Mid-Atlantic WITT Update

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

For those you you that have been involved in cell phone tracking, this might make some sense. The WITT (Wireless Intercept and Tracking Team) locates cell phones of subjects after the case agent has received a FEDERAL pen register order and the data has been *carefully* analyzed.

WITT Web Site

Be sure to bookmark the WITT web site on your computer[redacted]The site features contact information, cheat sheets, manuals, and other useful information.

b2
b7E

[redacted]Update

When using the[redacted]to track a[redacted]phone, be sure to get the[redacted]of the phone from the provider. Some providers are using[redacted]numbers for the phone in place of the traditional[redacted] The [redacted]is the actual phone number of the phone, but the system may use the[redacted]on the[redacted]portion of the call.

It is expected that[redacted]release a[redacted]version of the[redacted]this Fall.

[redacted]

b2
b7E

The[redacted]is a new product from[redacted]that allows portable tracking of[redacted]phones. It has one receiver, compared to the[redacted]in the[redacted]and looks like it will be a useful tool when we need to enter a building to pinpoint the exact location of a phone. We were able to find phones hidden in an office building and a hotel using the[redacted]during several different tests.

[redacted]Update

An upcoming update to the[redacted]will allow it to be connected to the[redacted]direction finding antenna array so that a bearing to the target can be obtained. It is unknown if we will need this capability if the[redacted]is updated to track[redacted]phones.

WITT Training

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 06-26-2007 BY 65179 DMH/TAM/KSR/cb

11/13/2006

b2
b7E

The WITT unit has finished the on-location regional training. A course is now offered at the Rte. 17 Fredricksburg Training Facility. It is called **"Wireless Intercept and Tracking (Course I)" :** A one-week refresher course taught by a contractor and Telecommunications Intercept & Collection Unit personnel. This course will provide an understanding of Wireless Intercept and Tracking Technologies in addition to focusing on operational training of the [redacted] technologies in both a classroom and a field environment. This course will be taught at the ERF. Eight students per class.

Course 2 should be the [redacted] course.

Check the Training Programs Unit web site for the new schedule: [redacted]

WFO will be conducting half-day training courses on the [redacted] as well as techniques for using test phones to map out specific sectors of cell sites.

b6
b7C

Cell Site Location Data

TICTU has posted some data on cell site locations from various providers. If you get updated lists please forward them to [redacted] at TICTU.

[redacted]

b2
b7E

DCS-3000 and the [redacted] Software

[redacted] software was added to the DCS-3000 pen register system that shows a map of the cell site and sector of the target. [redacted] allows you to look at historical data. These tools are already being used by the case agents and we should all be familiar with this software.

Cell site location data is not available for all providers and when no data is available, we need to revert to the old method of using a cell site list from the provider.

[redacted]
202 [redacted] Office
202 [redacted]

b6
b7C

SENSITIVE BUT UNCLASSIFIED

ATTACHED EXHIBITS
RESPONSE TO GOVERNMENT'S MEMORANDUM REGARDING LAW ENFORCEMENT PRIVILEGE AND REQUEST FOR AN EX PARTE AND IN CAMERA HEARING IF NECESSARY
CR08-814-PHX-DGC

↓ **EXHIBIT 35** ↓
↓ **EXHIBIT 35** ↓
↓ **EXHIBIT 35** ↓
↓ **EXHIBIT 35** ↓
↓ **EXHIBIT 35** ↓
↓ **EXHIBIT 35** ↓
↓ **EXHIBIT 35** ↓
↓ **EXHIBIT 35** ↓
↓ **EXHIBIT 35** ↓
↓ **EXHIBIT 35** ↓
↓ **EXHIBIT 35** ↓
↓ **EXHIBIT 35** ↓
↓ **EXHIBIT 35** ↓
↓ **EXHIBIT 35** ↓
↓ **EXHIBIT 35** ↓
↓ **EXHIBIT 35** ↓
↓ **EXHIBIT 35** ↓
↓ **EXHIBIT 35** ↓
↓ **EXHIBIT 35** ↓
↓ **EXHIBIT 35** ↓
↓ **EXHIBIT 35** ↓
↓ **EXHIBIT 35** ↓
↓ **EXHIBIT 35** ↓
↓ **EXHIBIT 35** ↓
↓ **EXHIBIT 35** ↓
↓ **EXHIBIT 35** ↓
↓ **EXHIBIT 35** ↓
↓ **EXHIBIT 35** ↓
↓ **EXHIBIT 35** ↓
↓ **EXHIBIT 35** ↓
↓ **EXHIBIT 35** ↓
↓ **EXHIBIT 35** ↓
↓ **EXHIBIT 35** ↓

FBI Response to EFF FOIA Request Nos. 1056287-000 & 1056307-1 (Aug. 27, 2007), *available at* <http://www.eff.org/files/filenode/061708CKK/082707_dcs06.pdf> (EFF PDF Set 6 of 6) (last accessed Jan. 11, 2011); (only relevant sections are included in this exhibit);

From: [redacted]
To:
Date: Wed, Jul 25, 2001 10:07 AM
Subject: Re: DCS3000 Tracker Software

b6
b7C

Sounds good [redacted] Can't wait to see it.

I was working with some agency guys yesterday. They are putting together a system with a flat panel ant. and a loggerhead and doing locations based on registrations. It works. They have a later software version on their loggerheads (I think). It will really help when we can use your software for real time display of the loggerhead activity. As it is, you have to make a pass in the area, move somewhere else, look at the log, etc. Any word on when Harris can make the change to the loggerhead?

>>> [redacted] 07/24 10:05 AM >>>
JP is finished with the software mods that support the multi-van [redacted] integration.

We are waiting delivery of the COM driver and the final approval of the [redacted]

b2
b6
b7C
b7E

EXHIBIT 36	Coast to Coast AM (website), *Lee Lapin - Guests - Coast to Coast AM*, Lee Lapin Biography, <http://www.coasttocoastam.com/guest/lapin-lee/6469> (last accessed Mar. 11, 2011);
EXHIBIT 36	
EXHIBIT 36	
EXHIBIT 36

Lee Lapin

Biography:

Lee Lapin works as a private detective, certified voice stress analyst, and is licensed as a surveillance consultant. He has written 23 books, that include six or seven on the fields of electronic surveillance, black bag entry techniques, physical surveillance, and personal intelligence gathering. He has produced a number of videos on these same subjects and has the capability to write, consult or demonstrate most of the latest techniques and equipment in both government and private arenas.

Websites:
- intelligencehere.com

Books:
- How to Get Anything on Anybody: Book 3
- How to Get Anything on Anybody: Book II
- Spygame: Winning Through Super Technology
- The Extreme Covert Catalogue
- Whole Spy Catalogue

Lee has worked with several agencies, both public and private, helping to develop surveillance and tracking equipment and techniques. His works ("letters on file") are employed as textbooks by many of the world's major intelligence agencies including the CIA, KGB and MOSSAD, the Justice Department, IRS, ATF, even the FBI. In addition, Lee has appeared on several national talk shows and has been featured on the front page of the NY Times, in People Magazine, Associated Press, and in many other magazines and newspapers.

Past Shows:

Surveillance & Privacy Invasion

Tuesday March 1, 2005

Private investigator and electronic engineer Lee Lapin (intelligencehere) shared the latest tricks and techniques of surveillance used by the worldâ€™s best agents and trackers. Optical surveillance, which is often legal, has had significant advancements in recent years. For instance, he cited how the DEA might set up a camera placed inside a plastic street cone to view through a person's window. Some cameras, he continued, have been reduced to the size of a dime and can go under doors or through a keyhole.In terms of audio surveillance, many new bugs are cell phone-based, said Lapin. If a person wanted to know if their phone was bugged, he suggested buying a second phone of the same model and taking both apart to see if there was anything extra in the suspected phone.He also talked about how private details about people are often culled through "pretexting," a now illegal method, where personal information is gained by someone under false pretenses. Lapin said he is cu ... More

Host: George Noory

- Geopolitical Disclosures - Shows
- Will the end of the world take place on May 21, 2011 as some groups believe? - Polls
- Enochian Magic & Crystal Skulls - Shows
- Electronic Harassment / Paranormal Techniques - Shows
- Serial Killers - Shows

Check out our calendar for George Noory's public appearances in 2011.

coasttocoastam

about 7 hours ago
Fish suffocate, die in Redondo Beach marina: Millions of fish were found dead in a Redondo Beach marina early ... http://bit.ly/dXBMM8

about 13 hours ago
News segment guest: Gerald Celente http://www.trendsresearch.com

about 18 hours ago
George Noory: Hey Coast Insiders, our first video chat tonight: http://tinyurl.com/C2CxChat 8pm PT; also my 1st hour guest is Alex Jones.

5:40 PM yesterday
UFO Mystery in Australia: Strange glowing

balls of light show up four nights in a row.
http://bit.ly/gJ1BUb

6:13 AM yesterday
News segment guests: Dr. Sherri Tenpenny
http://drtenpenny.com / Jerome Corsi

All Tweets

ATTACHED EXHIBITS
RESPONSE TO GOVERNMENT'S MEMORANDUM REGARDING LAW ENFORCEMENT PRIVILEGE
AND REQUEST FOR AN EX PARTE AND IN CAMERA HEARING IF NECESSARY
CR08-814-PHX-DGC

↓ **EXHIBIT 37** ↓
↓ **EXHIBIT 37** ↓
↓ **EXHIBIT 37** ↓
↓ **EXHIBIT 37** ↓
↓ **EXHIBIT 37** ↓
↓ **EXHIBIT 37** ↓
↓ **EXHIBIT 37** ↓
↓ **EXHIBIT 37** ↓
↓ **EXHIBIT 37** ↓
↓ **EXHIBIT 37** ↓
↓ **EXHIBIT 37** ↓
↓ **EXHIBIT 37** ↓
↓ **EXHIBIT 37** ↓
↓ **EXHIBIT 37** ↓
↓ **EXHIBIT 37** ↓
↓ **EXHIBIT 37** ↓
↓ **EXHIBIT 37** ↓
↓ **EXHIBIT 37** ↓
↓ **EXHIBIT 37** ↓
↓ **EXHIBIT 37** ↓
↓ **EXHIBIT 37** ↓
↓ **EXHIBIT 37** ↓
↓ **EXHIBIT 37** ↓
↓ **EXHIBIT 37** ↓
↓ **EXHIBIT 37** ↓
↓ **EXHIBIT 37** ↓
↓ **EXHIBIT 37** ↓
↓ **EXHIBIT 37** ↓
↓ **EXHIBIT 37** ↓
↓ **EXHIBIT 37** ↓
↓ **EXHIBIT 37** ↓
↓ **EXHIBIT 37** ↓

Excerpt of CDNRS files generated by the government's Pen/Trap device, *i.e.*, the SF-Martinez DCS-3000 server, while it was logging the government's surreptitious pings (*i.e.*, phone calls) made to the aircard;

11

9/11/09

FBI - Compact Disc Containing Real Time Cellular Tracking Data - No. 415-264-9596 - Dates 7/16/08 - Contains 3 Folders - Open Folder "CDNRS" With Microsoft Excel - Open Folders "Log" and "Sum" With Microsoft Notepad

FD-340 (Rev. 4-11-03)

File Number 288A-SX-82001-1A(94)

Field Office Acquiring Evidence SF | SJRA

Serial # of Originating Document 228

Date Received 4/2009

From SF Tech Unit
(Name of Contributor/Interviewee)

(Address)

(City and State)

By SA William Ng

To Be Returned ☐ Yes ☑ No

Receipt Given ☐ Yes ☑ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e) Federal Rules of Criminal Procedure

☐ Yes ☑ No

Federal Taxpayer Information (FTI)

☐ Yes ☐ No

Title: PLAZACABLE@SAFE-MAIL.NET;
IRS- VICTIM;
COMPUTER INTRUSION - CRIMINAL MATTER)

Reference:
(Communication Enclosing Material)

Description: ☐ Original notes re interview of

1 CD-ROM containing Real-time cellular tracking data of telephone # (415) 264-9596 on 7/26/2008

Location Area Code: Not available
IAPSystemIdentity: 40-3-1

Target Name: VERIZON
Target Number: 4152649596
DCS Call Number: 10
DCS Server Name: SF-Martinez Multiserver
DCS Connection Name: Verizon Wireless (SF)

CALL RELEASE MSC Call Number: 264039
Date: 07/16/2008
Time: 13:37:36.780
Location Area Code: 5-3
IAPSystemIdentity: 40-2-5

Target Name: VERIZON
Target Number: 4152649596
DCS Call Number: 11
DCS Server Name: SF-Martinez Multiserver
DCS Connection Name: Verizon Wireless (SF)

CALL TERMINATION ATTEMPT
MSC Call Number: 197795
Date: 07/16/2008
Time: 13:52:40.68
Called number: 4152649596
Calling number: 9253485566
Called Trunk Id:
Calling Trunk Id: 227-976
Called Esn:
IAPSystemIdentity: 40-3-1
IMSI:
IMEI:

Target Name: VERIZON
Target Number: 4152649596
DCS Call Number: 12
DCS Server Name: SF-Martinez Multiserver
DCS Connection Name: Verizon Wireless (SF)

CALL TERMINATION ATTEMPT
MSC Call Number: 329686
Date: 07/16/2008
Time: 13:52:41.86
Called number: 4152649596
Calling number: 9253485566
Called Trunk Id:
Calling Trunk Id: 48-1374
Called Esn: 050AF186
IAPSystemIdentity: 40-2-5
IMSI:
IMEI:

Target Name: VERIZON
Target Number: 4152649596
DCS Call Number: 11
DCS Server Name: SF-Martinez Multiserver
DCS Connection Name: Verizon Wireless (SF)

```
    CALL REDIRECTION
     MSC Call Number:            197795
     Redirected To:              4087819964
     Date:                       07/16/2008
     Time:                       13:52:40.729
     IAPSystemIdentity:          40-3-1


Target Name:           VERIZON
Target Number:         4152649596
DCS Call Number:       12
DCS Server Name:       SF-Martinez Multiserver
DCS Connection Name:   Verizon Wireless (SF)

    NETWORK SIGNAL
     Date:                       07/16/2008
     Time:                       13:52:44.405
     Call ID:                    329686
     IAPSystemIdentity:          40-2-5
     Alerting Signal:            Alerting Pattern 0
     Audible Signal:
     General Display:
     Called Number:
     Calling Number:
     Original Called Number:
     Last Redirecting Number:
     Redirecting Name:
     Redirecting Reason:
     Message Waiting Notif:
     Other:                      Private


Target Name:           VERIZON
Target Number:         4152649596
DCS Call Number:       11
DCS Server Name:       SF-Martinez Multiserver
DCS Connection Name:   Verizon Wireless (SF)

    CALL RELEASE     MSC Call Number:  197795
     Date:                       07/16/2008
     Time:                       13:53:55.849
     Location Area Code:         Not available
     IAPSystemIdentity:          40-3-1


Target Name:           VERIZON
Target Number:         4152649596
DCS Call Number:       12
DCS Server Name:       SF-Martinez Multiserver
DCS Connection Name:   Verizon Wireless (SF)

    CALL RELEASE     MSC Call Number:  329686
     Date:                       07/16/2008
     Time:                       13:53:56.625
     Location Area Code:         5-3
     IAPSystemIdentity:          40-2-5


Target Name:           VERIZON
Target Number:         4152649596
DCS Call Number:       13
DCS Server Name:       SF-Martinez Multiserver
DCS Connection Name:   Verizon Wireless (SF)
```

ATTACHED EXHIBITS

RESPONSE TO GOVERNMENT'S MEMORANDUM REGARDING LAW ENFORCEMENT PRIVILEGE AND REQUEST FOR AN EX PARTE AND IN CAMERA HEARING IF NECESSARY

CR08-814-PHX-DGC

↓ **EXHIBIT 38** ↓
↓ **EXHIBIT 38** ↓
↓ **EXHIBIT 38** ↓
↓ **EXHIBIT 38** ↓
↓ **EXHIBIT 38** ↓
↓ **EXHIBIT 38** ↓
↓ **EXHIBIT 38** ↓
↓ **EXHIBIT 38** ↓
↓ **EXHIBIT 38** ↓
↓ **EXHIBIT 38** ↓
↓ **EXHIBIT 38** ↓
↓ **EXHIBIT 38** ↓
↓ **EXHIBIT 38** ↓
↓ **EXHIBIT 38** ↓
↓ **EXHIBIT 38** ↓
↓ **EXHIBIT 38** ↓
↓ **EXHIBIT 38** ↓
↓ **EXHIBIT 38** ↓
↓ **EXHIBIT 38** ↓
↓ **EXHIBIT 38** ↓
↓ **EXHIBIT 38** ↓
↓ **EXHIBIT 38** ↓
↓ **EXHIBIT 38** ↓
↓ **EXHIBIT 38** ↓
↓ **EXHIBIT 38** ↓
↓ **EXHIBIT 38** ↓
↓ **EXHIBIT 38** ↓
↓ **EXHIBIT 38** ↓
↓ **EXHIBIT 38** ↓
↓ **EXHIBIT 38** ↓
↓ **EXHIBIT 38** ↓
↓ **EXHIBIT 38** ↓

USPIS Investigation Details Report Entry, USPIS Inspector James L. Wilson, RE: among other matters, a Stingray was used to locate the aircard; (Entry date: August 7, 2008); (ITEM NO. 5 of July 31, 2009 discovery set);

During the course of this investigation and conferring with TSD agents with the FBI and USPIS, we determined that doing a normal "Trap and Trace" on the aircard would suffice [redacted] Essentially we would ping the number associated to the card instead of collecting data from the aircard's connection.
On 7/10/08, an order was signed for a Trap and Trace on the suspect's aircard. On 7/14/08, Verizon provided historical tower data (the data was provided in compliance with a "2703D Order"). Tower data indicated that the suspect's aircard was hitting on four specific towers within the Santa Clara/San Jose area.
Based on this information, on 7/15/08, Agent Murray (FBI), Agent Medrano (IRS), Agent Fleischmann (IRS), Agent Daun (IRS) and I flew to Santa Clara/San Jose to start triangulating the suspect's position. Upon our arrival, we met with Agent William Ng at the San Jose FBI Office.
While at the San Jose Office, we met with several FBI agents with their Technical Service Division assigned to help use track the suspect's aircard. According to the TSD Agents, Verizon had a set-up problem with "Provisions" for the PEN data. Therefore, we were not able to get a signal on 7/15/08.
On 7/16/08, we were informed that they were able to track a signal and were using a "Stingray" to pinpoint the location of the aircard. After numerous of hours on surveillance, we were able to get a positive signal at an apartment complex in Santa Clara. The name of the complex is the "Domicilio" Apartments located at 431 El Camino Real, Santa Clara, CA 95050. We were able to narrow down the signal to three possible apartments: #1120, #1122 and #1124. This apartment complex is across the street from Santa Clara University.
On 7/17/08, Agent Medrano and I went to the carrier annex while the other agents did other tasks. The carrier was able to provide the names of all the occupants of the perspective units. At that time, I notified Inspector Quan Howard (T/L, San Jose Office). Inspector Howard met me at a location near campus. He notified a Santa Clara PD contact who was able to provide us with utilities (The utilities for the complex are provided by the city of Santa Clara) for each apartment. Each occupant had a California Driver's License number with their name.
When I ran the occupants' names through the CA DMV and the DL number for the occupant of #1122 did not match. The occupant's name for #1122 is Steven Travis Brawner (the DL number given comes back to a female). I went to the Domicilio Apartments and met with the apartment manager, Mona Chen. I served a subpoena on the Domicilio Apartments for the rental agreement/file for unit #1122 (and the other two units too so I would not arise suspicion for that specific unit. And because we weren't completely sure which unit it was at the time).
When I received the application for unit #1122, the handwriting on the rental agreement of the occupant looked very similar to the handwriting on the fraudulent PO Box applications in the name of Patrick Stout and Edward Berner. A copy of the occupant's driver's license was in the file too. The subject in the photo was a white male in his twenties. It was also determined that the social security number that the suspect provided on the application (SSN #559-87-4167) does belong to a Steven Travis Brawner who has been deceased for over 10 years!
Over the next two days we were out there trying to establish if anyone actually lives in that unit. Due to the intelligence and paranoia of our suspect, we had/have real concerns if the suspect lives there or this location is a drop/stage location. On 7/22/08, we were able to secure a Search Warrant in the Northern District of California for 431 El Camino Real, #1122, Santa Clara, Ca 95050. To this date, we have not served it yet because it may be necessary to do another controlled delivery of money from the CI to the suspect next week.
It should be noted that while out in San Jose/Santa Clara, I received subpoenaed information from Bullion Direct. Back in May 08', our suspect opened an account with Bullion Direct in the name of Patrick Stout (the same name that was used to pick up the 68K package we sent to the suspect on May 7, 2008). Bullion Direct is an "Egold" exchange company.
I was able to identify this Bullion Direct account because the suspect used a fraudulent debit card to purchase Postal money orders in southern California. When I retrieved the money order images, they were made payable to Bullion Direct. Bullion Direct provided me with payment history and shipment history. Interestingly enough, right after our suspect received his $68,000.00, he left the Santa Clara/San Jose area, went to southern California and purchased numerous Postal money Orders (indicated by the dates on the money order copies provided by Bullion Direct to purchase gold. Furthermore, Bullion Direct mailed two gold shipments (via FedEx) in late May/June to a Patrick Stout to the same FedEx/Kinkos (249 S. California Ave., Palo Alto, Ca) that we sent the original $68,000.
On 7/23/08, the suspect was indicted on a 50 count indictment in the District of Arizona for Mail fraud, Aggravated ID Theft, Access Devices, Wire Fraud, Tax Fraud and Conspiracy to Defraud the Government. Due to the suspect's anonymity, I will be unable to enter the suspect into ISIIS until he is arrested.

Event ID: 5560190	**FY:** 2008
Credited Inspector: USPIS\JLWilson	**Nick Name:** surveillance and arrest of suspect
Entered By : USPIS\JLWilson	**Entered Date:** 08/07/2008

EXHIBIT 39

EXHIBIT 39
EXHIBIT 39
EXHIBIT 39

>$6,000 mo Credit Report if self employed - last yrs tax Return
Rent = $1800 - $2500/mo

~~7-15-08~~ ~~Domicilio Apartments~~ Bldg 1 ? ↑ (Return)
431 El Camino Real 3 Apts
Santa Clara, CA 95050 1120 | 1122 | 1124

Post office - John Sanchez Carrier Annex
[redacted] (contact #)

Ford Pick Up CA 6Z51192
possible suspect - photos taken

Santa Clara PD - didn't have anything

male in teal shirt watching bball game
- entered bdg 2

Utility Search - power, internet, - PG&E - Apt. Complexes have seperate utility companies
✓ tax return search
✓ Post office - verifying forwarding info
Run plates
Review Video
✓ Accurint
Sting Ray

[redacted] (Phone #)

EXHIBIT 40	Paper print-out of email sent from IRS-CI Agent Tracy L. Daun to Jeffrey H. Willert, Re: among other matters, IRS-CI Agent Daun's request to be present and to assist the FBI with triangulating the aircard location; (Email sent date: July 11, 2008 11:16am); (ITEM NO. 3 of September 24, 2010 discovery set);
EXHIBIT 40	
EXHIBIT 40	
EXHIBIT 40

Special Agent, CIS
IRS-CI
[redacted]
Phoenix AZ
[redacted]

From: Willert Jeffrey H
Sent: Friday, July 11, 2008 11:20 AM
To: Daun Tracy L
Subject: RE: Bulk Filing Case

Hey Tracy,
[redacted]
Take care,
Jeff

→ communication Re logistics.

Jeffrey H. Willert
SSA - CIS, Southern Pacific Area
[redacted]
IRS - CI - Electronic Crimes Program
[redacted]

From: Daun Tracy L
Sent: Friday, July 11, 2008 11:16 AM
To: Willert Jeffrey H
Subject: Bulk Filing Case

→ Again a generic use of the term.

CI-2 / Carter

Jeff,

Do you mind if I travel with the case agents next week for the [redacted] investigation, even prior to the warrant. FBI will be triangulating down on the "hackers" Verizon Wireless Broadband card and I'd like to see how that works and be available to assist with what I can. I also thought that it would be good if I was there, in case we ended up moving on the warrant quicker than anticipated.

After many delays with Northern CA's USAO (and a slight hiccup due to having some data through the wrong channels), we **think** they are finally going to take our court orders before the magistrate today. [redacted]

← prospective logistics

[redacted] Based on recent

→ this relates to the materials initially received via subpoena. This is addressed in court documents

information, I think we will only run into one laptop - so it probably isn't necessary to have any additional help.

Thanks!

Tracy L. Daun
Special Agent, CIS
IRS-CI
[redacted]
Phoenix AZ
[redacted]

ATTACHED EXHIBITS
RESPONSE TO GOVERNMENT'S MEMORANDUM REGARDING LAW ENFORCEMENT PRIVILEGE
AND REQUEST FOR AN EX PARTE AND IN CAMERA HEARING IF NECESSARY
CR08-814-PHX-DGC

↓ **EXHIBIT 41** ↓
↓ **EXHIBIT 41** ↓
↓ **EXHIBIT 41** ↓
↓ **EXHIBIT 41** ↓
↓ **EXHIBIT 41** ↓
↓ **EXHIBIT 41** ↓
↓ **EXHIBIT 41** ↓
↓ **EXHIBIT 41** ↓
↓ **EXHIBIT 41** ↓
↓ **EXHIBIT 41** ↓
↓ **EXHIBIT 41** ↓
↓ **EXHIBIT 41** ↓
↓ **EXHIBIT 41** ↓
↓ **EXHIBIT 41** ↓
↓ **EXHIBIT 41** ↓
↓ **EXHIBIT 41** ↓
↓ **EXHIBIT 41** ↓
↓ **EXHIBIT 41** ↓
↓ **EXHIBIT 41** ↓
↓ **EXHIBIT 41** ↓
↓ **EXHIBIT 41** ↓
↓ **EXHIBIT 41** ↓
↓ **EXHIBIT 41** ↓
↓ **EXHIBIT 41** ↓
↓ **EXHIBIT 41** ↓
↓ **EXHIBIT 41** ↓
↓ **EXHIBIT 41** ↓
↓ **EXHIBIT 41** ↓
↓ **EXHIBIT 41** ↓
↓ **EXHIBIT 41** ↓
↓ **EXHIBIT 41** ↓
↓ **EXHIBIT 41** ↓

Letter from AUSA Frederick Battista to Daniel Rigmaiden, RE: among other matters, use of a mobile tracking device to locate the aircard; (Postmark date: June 18, 2010); (only relevant sections are included in this exhibit);

U.S. Department of Justice

United States Attorney
District of Arizona
Two Renaissance Square
40 North Central, Suite 1200
Phoenix, Arizona 85004-4408

Official Business
Penalty for Private Use $300

ADDRESS SERVICE REQUESTED

Daniel Rigmaiden
Agency No. 10966111
CCA-CADC
Post Office Box 6300
Florence, Arizona 85132

US OFFICIAL MAIL
$300 Penalty
For Private Use

049J00743196
$00.44⁰
06/18/2010
Mailed From 85004
US POSTAGE

JUN 21 2010

85132863OO 2902

U.S. Department of Justice

United States Attorney
District of Arizona

Two Renaissance Square
40 North Central Avenue, Suite 1200
Phoenix, Arizona 85004-4408

Main: (602) 514-7500
Main Fax: (602) 514-7693

May 27, 2010

Daniel Rigmaiden
Agency No. 10966111
CCA-CADC
Post Office Box 6300
Florence, Arizona 85132

Re: United States v. Daniel David Rigmaiden
CR-08-814-PHX-DGC

Dear Mr. Rigmaiden:

[redacted]

J. "Triangulation"

With respect to Postal Inspector Wilson's use of the term "triangulation" in his report, please be advised that he used this term as a figure of speech and not a technical term. In addition, with respect to the use of any mobile tracking device, no triangulation was done through the use of multiple devices.

[redacted]

Sincerely yours,

DENNIS K BURKE
United States Attorney
District of Arizona

FREDERICK A. BATTISTA
Assistant United States Attorney

cc: Phillip Seplow
Shadow Counsel for Defendant Daniel David Rigmaiden

Taylor Fox
Counsel for Defendant Ransom Carter

ATTACHED EXHIBITS
RESPONSE TO GOVERNMENT'S MEMORANDUM REGARDING LAW ENFORCEMENT PRIVILEGE
AND REQUEST FOR AN EX PARTE AND IN CAMERA HEARING IF NECESSARY
CR08-814-PHX-DGC

↓ **EXHIBIT 42** ↓
↓ **EXHIBIT 42** ↓
↓ **EXHIBIT 42** ↓
↓ **EXHIBIT 42** ↓
↓ **EXHIBIT 42** ↓
↓ **EXHIBIT 42** ↓
↓ **EXHIBIT 42** ↓
↓ **EXHIBIT 42** ↓
↓ **EXHIBIT 42** ↓
↓ **EXHIBIT 42** ↓
↓ **EXHIBIT 42** ↓
↓ **EXHIBIT 42** ↓
↓ **EXHIBIT 42** ↓
↓ **EXHIBIT 42** ↓
↓ **EXHIBIT 42** ↓
↓ **EXHIBIT 42** ↓
↓ **EXHIBIT 42** ↓
↓ **EXHIBIT 42** ↓
↓ **EXHIBIT 42** ↓
↓ **EXHIBIT 42** ↓
↓ **EXHIBIT 42** ↓
↓ **EXHIBIT 42** ↓
↓ **EXHIBIT 42** ↓
↓ **EXHIBIT 42** ↓
↓ **EXHIBIT 42** ↓
↓ **EXHIBIT 42** ↓
↓ **EXHIBIT 42** ↓
↓ **EXHIBIT 42** ↓
↓ **EXHIBIT 42** ↓
↓ **EXHIBIT 42** ↓
↓ **EXHIBIT 42** ↓
↓ **EXHIBIT 42** ↓

Letter from AUSA Frederick Battista to Daniel Rigmaiden, RE: among other matters, the equipment used to locate the aircard is a “pen register trap and trace device” and not a “tracking device”; (Letter date: September 8, 2010); (only relevant sections are included in this exhibit);

U.S. Department of Justice

United States Attorney
District of Arizona

Two Renaissance Square
40 North Central Avenue, Suite 1200
Phoenix, Arizona 85004-4408

Main: (602) 514-7500
Main Fax: (602) 514-7693

September 8, 2010

Daniel Rigmaiden
Agency No. 10966111
CCA-CADC
Post Office Box 6300
Florence, Arizona 85132

Re: United States v. Daniel David Rigmaiden
CR-08-814-PHX-DGC

Dear Mr. Rigmaiden:

1. This is in response to your request for an unredacted copy of the e-mail from IRS-CI Supervisory Special Agent Albert A. Childress to IRS-CI Tax Fraud Investigative Assistant Toni D. Stewart and Special Agent Denise Medrano, dated July 17, 2008, at 8:10 AM. In particular, the relevant sentence reads as follows "FBI does not want to disclose the XXXX [explanatory insert - tracking device] (understandably so)." (Parenthetical in original document.) Please be advised that the e-mail discusses, in generic terms, the pen register trap and trace device that was used to locate the subject aircard. Again, at this point, the government is only willing to advise you that a "pen register trap and trace device" (what we have been previously been referring to as the "tracking device") was used to locate the subject aircard. Supervisory Special Agent Childress had no role in the actual operation of the equipment.

Sincerely yours,

DENNIS K BURKE
United States Attorney
District of Arizona

FREDERICK A. BATTISTA
Assistant United States Attorney

Enclosures

cc: Philip Seplow
Shadow Counsel for Defendant Daniel David Rigmaiden

Taylor Fox
Counsel for Defendant Ransom Carter

EXHIBIT 43	Letter from AUSA Frederick A. Battista to Daniel Rigmaiden, RE: Stingray is a generic term; (Letter date: November 23, 2010);
EXHIBIT 43	
EXHIBIT 43	
EXHIBIT 43

U.S. Department of Justice

United States Attorney
District of Arizona

Two Renaissance Square
40 North Central Avenue, Suite 1200
Phoenix, Arizona 85004-4408

Main: (602) 514-7500
Main Fax: (602) 514-7693

November 23, 2010

Daniel Rigmaiden
Agency No. 10966111
CCA-CADC
Post Office Box 6300
Florence, Arizona 85132

Re: United States v. Daniel David Rigmaiden
CR-08-814-PHX-DGC

Dear Mr. Rigmaiden:

This is in response to your renewed request for additional discovery, dated November 11, 2010, regarding the use of the term "stingray" in this case. I apologize for not realizing that this issue had been tangentially addressed in earlier exchanges. By our count, this is the 58th discovery related letter that has been sent to you or one of your prior attorneys in this case. For purposes of this case as of this date, please be advised that whenever the term "stingray" appears in the discovery, the case agents, including IRS-CI Special Agents Denise Medrano, Michael Fleischmann and Tracy Daun, FBI Special Agent Richard Murray and Postal Inspector James Wilson, as well as any of their immediate supervisors, were simply using the term in a generic sense and were not specifically referring to any particular piece of equipment that may have actually been used to locate the subject aircard.

Sincerely yours,

DENNIS K BURKE
United States Attorney
District of Arizona

FREDERICK A. BATTISTA
Assistant United States Attorney

cc: Philip Seplow
Shadow Counsel for Defendant Daniel David Rigmaiden

Taylor Fox
Counsel for Defendant Ransom Carter

EXHIBIT 44

EXHIBIT 44
EXHIBIT 44
EXHIBIT 44

ELECTRONIC FRONTIER FOUNDATION

DECEMBER 1ST, 2009

Surveillance Shocker: Sprint Received 8 MILLION Law Enforcement Requests for GPS Location Data in the Past Year

News Update by *Kevin Bankston*

This October, Chris Soghoian — computer security researcher, oft-times journalist, and current technical consultant for the FTC's privacy protection office — attended a closed-door conference called "ISS World". ISS World — the "ISS" is for "Intelligence Support Systems for Lawful Interception, Criminal Investigations and Intelligence Gathering" — is where law enforcement and intelligence agencies consult with telco representatives and surveillance equipment manufacturers about the state of electronic surveillance technology and practice. Armed with a tape recorder, Soghoian went to the conference looking for information about the scope of the government's surveillance practices in the US. What Soghoian uncovered, as he reported on his blog this morning, is more shocking and frightening than anyone could have ever expected

At the ISS conference, Soghoian taped astonishing comments by Paul Taylor, Sprint/Nextel's Manager of Electronic Surveillance. In complaining about the volume of requests that Sprint receives from law enforcement, Taylor noted a shocking number of requests that Sprint had received in the past year for precise GPS (Global Positioning System) location data revealing the location and movements of Sprint's customers. That number?

EIGHT MILLION.

Sprint received over 8 million requests for its customers' information in the past 13 months. That doesn't count requests for basic identification and billing information, or wiretapping requests, or requests to monitor who is calling who, or even requests for less-precise location data based on which cell phone towers a cell phone was in contact with. That's *just GPS*. And, that's not including legal requests from civil litigants, or from foreign intelligence investigators. That's *just law enforcement*. And, that's not counting the few other major cell phone carriers like AT&T, Verizon and T-Mobile. That's *just Sprint*.

Here's what Taylor had to say; the audio clip is here and we are also mirroring a zip file from Soghoian containing other related mp3 recordings and documents.

> *[M]y major concern is the volume of requests. We have a lot of things that are automated but that's just scratching the surface. One of the things, like with our GPS tool. We turned it on the web interface for law enforcement about one year ago last month, and we just passed 8 million requests. So there is no way on earth my team could have handled 8 million requests from law enforcement, just for GPS alone. So the tool has just really caught on fire with law enforcement. They also love that it is extremely inexpensive to operate and easy, so, just the sheer volume of requests they anticipate us automating other features, and I just don't know how we'll handle the millions and millions of requests that are going to come in.*

Eight million would have been a shocking number even if it had included every single legal request to every single carrier for every single type of customer information; that Sprint alone received eight million requests just from law enforcement only for GPS data is absolutely mind-boggling. We have long warned that cell phone tracking poses a threat to locational privacy, and EFF has been fighting in the courts for years to ensure that the government only tracks a cell phone's location when it has a search warrant based on probable cause. EFF has also complained before that a dangerous level of secrecy surrounds law enforcement's communications surveillance practices like a dense fog, and that without stronger laws requiring detailed reporting about how the government is using its surveillance powers, the lack of accountability when it comes to the government's access to information through third-party phone and Internet service providers will necessarily breed abuse. But we never expected such huge numbers to be lurking in that fog.

Now that the fact is out that law enforcement is rooting through such vast amounts of location data, it raises profoundly important questions that law enforcement and the telcos must answer:

- How many innocent Americans have had their cell phone data handed over to law enforcement?
- How can the government justify obtaining so much information on so many people, and how can the telcos justify handing it over?
- How did the number get so large? Is the government doing massive dragnet sweeps to identify every single cell phone that was in a particular area at a particular time? Is the government getting location information for entire "communities of interest" by asking not only for their target's location, but also for the location of every person who talked to the target, and every person who talked to them?

- Does the number only include requests to track phones in real-time, or does it include requests for historical GPS data, and if so, why did the telcos have that incredibly sensitive data sitting around in the first place? Exactly when and how are they logging their users' GPS data, and how long are they keeping that data?
- What legal process was used to obtain this information? Search warrants? Other court orders? Mere subpoenas issued by prosecutors without any court involvement? How many times was this information handed over without any legal process at all, based on government claims of an urgent emergency situation?
- Looking beyond Sprint and GPS, how many Americans have had their private communications data handed over to law enforcement by their phone and Internet service providers?
- What exactly has the government done with all of that information? Is it all sitting in an FBI database somewhere?
- Do you really think that this Orwellian level of surveillance is consistent with a free society and American values? *Really*?

These questions urgently need to be asked — by journalists, and civil liberties groups like EFF, and by every cell phone user and citizen concerned about privacy. Most importantly, though, they must be asked by Congress, which has failed in its duty to provide oversight and accountability when it comes to law enforcement surveillance. Congress should hold hearings as soon as possible to demand answers from the government and the telcos under oath, and clear the fog so that the American people will finally have an accurate picture of just how far the government has reached into the private particulars of their digital lives.

Even without hearings, though, the need for Congress to update the law is clear. At the very least, Congress absolutely must stem the government's abuse of its power by:

- Requiring detailed reporting about law enforcement's access to communications data using the Electronic Communications Privacy Act (ECPA), just as it already requires for law enforcement wiretapping under the Wiretap Act, and make sure that the government actually fulfills its obligations rather than ignore the law for years on end.
- Requiring that the government "minimize" the communications data it collects under ECPA rather than keep it all forever, just like it is supposed to do with wiretaps.
- Prohibiting the government from using in a criminal trial any electronic communications content or data that it obtains in violation of ECPA, just as the government is prohibited by the Wiretap Act from using illegally acquired telephone intercepts.
- Clarifying that ECPA can only be used to get specific data about particular individuals and cannot be used for broad sweeps, whether to identify everyone in a particular geographic area or to identify every person that visits a particular web site.

It's time for Congress to pull the curtain back on the vast, shadowy world of law enforcement surveillance and shine a light on these abuses. In the meantime, we give our thanks to those like Chris Soghoian who are doing important work to uncover the truth about government spying in America.

UPDATE: Sprint has responded to Soghoian's report:

> *The comments made by a Sprint corporate security officer during a recent conference have been taken out of context by this blogger. Specifically, the "8 million" figure, which the blogger highlights in his email and blog post, has been grossly misrepresented. The figure does not represent the number of customers whose location information was provided to law enforcement, as this blogger suggests.*
>
> *Instead, the figure represents the number of individual "pings" for specific location information, made to the Sprint network as part of a series of law enforcement investigations and public safety assistance requests during the past year. It's critical to note that a single case or investigation may generate thousands of individual pings to the network as the law enforcement or public safety agency attempts to track or locate an individual.*
>
> *Instances where law enforcement agencies seek customer location information include exigent or emergency circumstances such as Amber Alert events, criminal investigations, or cases where a Sprint customer consents to sharing location information.*
>
> *Sprint takes our customers' privacy extremely seriously and all law enforcement and public safety requests for customer location information are processed in accordance with applicable state and federal laws.*

This response provides some important answers, while raising even more questions. First off, Sprint has confirmed that it received 8 million requests, while denying a charge that no one has made: that 8 million individual customers' data was handed over. Sprint's denial also begs the question: how many individual customers *have* been affected?

As for Sprint's claim that in some instances a single case or investigation may generate thousands of location "pings", that is certainly possible, but that doesn't make the 8 million number any less of a concern, or moot any of the important questions raised by Soghoian in his report or by EFF in its post regarding the lack of effective oversight and transparency in this area.

Even assuming that Sprint's statement about "pings" is true, 8 million — or, in other words, 8,000 thousands — is still an astronomical number and more than enough to raise serious concerns that Congress should investigate and address. Moreover, the statement raises additional questions: exactly what legal process is being used to authorize the multiple-ping surveillance over time that Sprint is cooperating in? Is Sprint demanding search warrants in those cases? How secure is this automated interface that law enforcement is using to "ping" for GPS data? How does Sprint insure that only law enforcement has access to that data, and only when they have appropriate legal process? How many times has Sprint disclosed information in "exigent or emergency circumstances" without any legal process at all? And most worrisome and intriguing: what customers does Sprint think have "consent[ed] to the sharing [of] location data" with the government? Does Sprint think it is free to hand over the information of anyone who has turned on their GPS functionality and shared information with Sprint for location-based services? Or even the data of anyone who has agreed to their terms of service? What *exactly* are they talking about?

These questions are only the beginning, and Sprint's statement doesn't come close to answering all of them. Of course, we appreciate that Sprint has begun a public dialogue about this issue. But this should be only the beginning of that discussion, not the end. Ultimately, the need for Congress to investigate the true scope of law enforcement's communications surveillance practices remains. Congress can and should dig deeper to get the hard facts for the American people, rather than forcing us to rely solely on Sprint's public relations office for information on these critical privacy issues.

Related Issues: *Cell Tracking*, *Locational Privacy*

[Permalink: http://www.eff.org/deeplinks/2009/12/surveillance-shocker-sprint-received-8-million-law]

Want to learn how you can defend free speech, stand up for privacy, fight for government transparency, support consumer rights, and protect your right to innovation in the digital world? Visit **http://eff.org/fight** to find ways to help.

EXHIBIT 45
EXHIBIT 45
EXHIBIT 45

<< Back to Article

FBI E-Mail Shows Rift Over Warrantless Phone Record Grabs

By Ryan Singel 12.20.07

By now it's well known that FBI agents can't always be troubled to get a court order before going after a surveillance target's telephone and internet records. But newly released FBI documents show that aggressive surveillance tactics have even caused friction within the bureau.

"We deal mostly with the fugitive squad here, and, like in many other offices, these guys have a reputation for cutting corners," a surveillance specialist at the FBI's Minneapolis field office complained in an internal e-mail last year. "I'm not bashing them; it's the way they do business. Getting a court order is the absolute last step, if they have to.

"Before I had a blowup with a particular agent ... we were constantly asked to call our contacts at service providers to see if we could get various information without having to get a court order," the message continues. "This gets old, believe me. ... Doing this once or twice to help out turns into SOP (standard operating procedure) ... It's expected, and you're criticized as a tech agent if you refuse to do this later on."

The revelation is the second this year showing that FBI employees bypassed court order requirements for phone records. In July, the FBI and the Justice Department Inspector General revealed the existence of a joint investigation into an FBI counter-terrorism office, after an audit found that the Communications Analysis Unit sent more than 700 fake emergency letters to phone companies seeking call records. An Inspector General spokeswoman declined to provide the status of that investigation, citing agency policy.

The June 2006 e-mail (.pdf) was buried in more than 600-pages of FBI documents obtained by the Electronic Frontier Foundation, in a Freedom of Information Act lawsuit.

The message was sent to an employee in the FBI's Operational Technology Division by a technical surveillance specialist at the FBI's Minneapolis field office -- both names were redacted from the documents. The e-mail describes widespread attempts to bypass court order requirements for cellphone data in the Minneapolis office.

Remarkably, when the technical agent began refusing to cooperate, other agents began calling telephone carriers directly, posing as the technical agent to get customer cellphone records.

Federal law prohibits phone companies from revealing customer information unless given a court order, or in the case of an emergency involving physical danger.

The documents are the second batch released by the EFF after winning a Freedom of Information Act lawsuit last May. The first set of documents shed light on the breadth and sophistication of the FBI's national wiretapping system, which is wired into telecom switches around the United States under the terms of the 1994 Communications Assistance for Law Enforcement Act -- a law that was extended to broadband internet switches in May of this year.

The new documents detail how a little-known FBI telephone intercept unit has developed a powerful cellphone tracking technology that agents use to monitor the physical movements of surveillance targets, even on phones that are not GPS equipped.

Originally developed to capture and arrest computer hacker Kevin Mitnick in 1995, the system today relies on a mobile FBI van that has access to a wireless carrier's cell site tracking information in real time. A special surveillance unit called the Wireless Intercept and Tracking Team (WITT) operates the van, using the cell site location to get to the approximate location of the cellphone customer, then uses direction-finding gear to zero in on the target.

The technical agent complained in the e-mail that FBI agents looking for a suspect tend to skip gumshoe investigative techniques in favor of the slick tracking van. "These guys always want to take the WITT vehicle out and drive around half of town (sic) to find the guy," the agent wrote.

The tracking system is part of the FBI's Digital Collection System, or DCS, a suite of software packages used for criminal and intelligence phone taps, which relies on a massive interlinked fiber-optic network that connects surveillance terminals around the country.

In brief, the mobile tracking system works as follows:

FBI agents investigating a case prepare a court order saying a cellphone number is likely relevant to an ongoing investigation, and a judge signs off on it.

The court order is faxed to a mobile carrier, which then turns on surveillance in its switches, and begins delivering call data and cell site information to the FBI's DCS 3000 software.
That software keeps track of which cellphone towers a phone uses or pings. A central FBI database translates a mobile carrier's cell tower code to latitude and longitude coordinates.
The software sends the coordinates to the agents and technical personnel in the mobile unit who then drive to the general area. But since cell tower information is not precise, agents in the van use antenna array connected to tracking software to zero in on the cellphone.
The FBI's technology office trumpeted the tracking function of the DCS 3000 software in a letter to the FBI director, boasting that it was used after a December 2005 North Carolina kidnapping to help find the victim unharmed.

Justice Department spokesman Dean Boyd says the department's policy allows the FBI to get cell tower information using under the low legal standard that applies to monitoring the digits a phone customer dials. Under that "pen register" standard, the FBI need only assert that the surveillance is relevant to an investigation -- the target need not be suspected of a crime.

When GPS-level data is wanted, law enforcement agents still need to show probable cause to a judge, said Boyd, who deferred questions about the Minneapolis agent's e-mail to the FBI.

FBI spokesman Paul Bresson cautioned against drawing conclusions from redacted government documents, and claimed that the FBI follows the law.

"FBI agents are trained to enforce the law using all available legal tools," Bresson said. "Absent an emergency circumstance involving danger or death or serious physical injury, the FBI does not request, nor do service providers give, any records without a court order."

The FBI tech agent's critical e-mail is best understood in light of the bureau's ongoing courtroom attempts to get cellphone location information without having to show probable cause, according to EFF lawyer Marcia Hofmann.

"For years the government has made dubious legal claims to justify tracking people's locations with minimal oversight," Hofmann said. "These docs show that the government hasn't satisfied its own weak standards in some cases."

Other revelations in the document include:

National security wiretaps in a Florida investigation captured more than 1,800 phone conversations, and led to 50 international terrorism advisories. Though details are redacted from the document, that case appears to be the so-called Liberty City Seven. Prosecutors initially trumpeted that the seven men were plotting to blow up the Sears Tower, though a government official later admitted the group was "more aspirational than operational." Last week a Florida jury acquitted one man and failed to reach a verdict on the other six.
In 2006, DCS 5000, the FBI's national security wiretapping software, captured 27,728,675 communication sessions. The document does not define what a "session" consists of. That year the FBI reported winning 2,176 FISA, or Foreign Intelligence Surveillance Act, warrants from a secret court.
By 2003 one cellphone carrier, Richmond, Virginia-based Triton PCS, was handling some 1,800 subpoenas and court orders a year. With 800,000 customers, that represented one records demand for every 444 customers.
The FBI uses a Raytheon-developed tool known as the Digital Multimedia Watchdog to record and store phone calls and internet communications between informants and targets of an investigation. That tool can "collect, process and store large amounts of multimedia data, including voice, fax, data and video."
DCS 3000 -- the FBI's tool for recording the phone numbers a target calls, or is called from -- was set loose on 5,300 phones in 2005, at a cost of $320 per targeted number. Those costs did not include payments to telecoms for the intercepts.
The software is maintained by Booz Allen Hamilton and contained more than 490,000 lines of code as of 2005.
The three software components of the FBI's phone surveillance system cost $38.7 million in 2003 and $39 million in 2004.
Computers running these software packages at FBI offices and surveillance locations are connected through a Sprint-run closed fiber-optic network that allows surveillance to continue even when offices are destroyed, as happened during Sept. 11 and Hurricane Katrina.