



U.S. Department of Justice

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

Requester: Catherine Crump Request Number: 07-4123

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

Dear Requester:

22 OCT 2009

This is in further response to your request for records under the Freedom of Information Act. Although, the EOUSA does not consider the Hodor Declaration responsive to your request, it has nonetheless reviewed it for discretionary release under the terms of the Attorney General's March 19, 2009 Memorandum on the FOIA. This document originated with the Federal Bureau of Investigation (FBI); therefore, in accordance with Department of Justice regulations, the EOUSA has consulted with the FBI. The FBI and EOUSA have determined after conducting a foreseeable harm analysis that this document could be disclosed in part without resulting in harm to an interest protected by one of the FOIA statutory exemptions.

This letter constitutes a partial release of the 28-page Hodor Declaration. The EOUSA is withholding Exhibit 1 to the Declaration in its entirety, consisting of 12 pages, as well as references to that exhibit within the Declaration, under Exemption 4, as it is material copyrighted by a third party. See Hodor Decl. at 3 n.3. The EOUSA is also withholding portions of the Declaration under Exemptions 6 and 7(C) that contain personally identifying information about the declarant.

Enclosed please find:

- 17 page(s) are being released in full (RIF);
- 11 page(s) are being released in part (RIP);
- 12 page(s) are withheld in full (WIF) and

The exemptions cited are marked below. An enclosure to this letter explains the exemptions in more detail.

Section 552

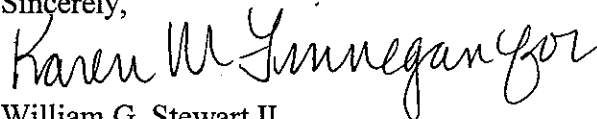
Section 552a

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

Although I am aware that this request is the subject of ongoing litigation and that appeals are not ordinarily acted on in such situations, I am required by statute and regulation to inform you that if

you consider my response to be a denial of your request, you have the right to file an administrative appeal by writing within 60 days from the date of this letter to the **Office of Information Policy, United States Department of Justice, 1425 New York Avenue, Suite 11050, Washington, D.C. 20530-0001.**

Sincerely,



William G. Stewart II

Assistant Director

Enclosure(s)

DECLARATION OF HENRY HODOR

HENRY HODOR affirms as follows under penalty of perjury:

1. I am [b7c] [b7c] telecommunications firm that performs consulting services for the Federal Bureau of Investigation ("FBI"). The discussion below is based upon my training and experience in the telecommunications industry, my review of documents provided to me in the course of consulting for the FBI, information provided to me by personnel whom I supervise, and persons employed in the wireless telephone industry and by law enforcement.

2. I make this declaration having been duly advised that the government will offer it in support of a request for authorization to use a pen register and trap and trace device (pen/trap) linked to an access point within a service provider's network to enable the capture of recorded information identifying (i) the base station tower(s) and sector(s) with which a subject wireless telephone was in contact at the beginning and/or end of a call and (ii) the mobile switching center (MSC) serving that telephone (collectively, "the SUBJECT TOWER/SECTOR & MSC RECORDS"). I make this declaration for the limited purpose of demonstrating that (a) service providers generate and store the SUBJECT TOWER/SECTOR & MSC RECORDS for their own network and

business reasons, regardless of regulatory obligation or specific request by law enforcement; and accordingly; (b) the SUBJECT TOWER/SECTOR & MSC RECORDS are only available to law enforcement after a service provider has for its own reasons generated and stored them at least temporarily; and (c) while the SUBJECT TOWER/SECTOR & MSC RECORDS establish the general vicinity of a wireless telephone at the beginning and/or end of a call, they do not establish the telephone's location with precision.

A. Experience and Training

3. 

b7C

D.¹ Since becoming a telecommunications consultant

¹ CALEA, Pub. L. No. 103-414, 108 Stat. 4279.

in August 1996, I have worked under contract to the FBI, assisting its efforts to implement CALEA.²

4. During my tenure at [b7c] I worked extensively with cellular telephone networks. From 1991 until approximately 1995, [b7c]

[b7c] These courses emphasized wireless telephone technology, including the inner workings of call-processing within cellular networks. I applied this training and was further educated about cellular networks during network engineering assignments. [b7c] network engineers, including me, were responsible for designing and implementing facilities throughout the New York City metropolitan area that connected [b7c] network with, among other entities, wireless carriers, interexchange carriers and paging companies. Moreover, [b7c]

[b7c] I relied extensively on [b7c] network engineers, including me, to assist it in solving design, topology, engineering, signaling, and interconnection issues relating to wireless telephone service.

² CALEA designates the Attorney General of the United States as the senior federal law enforcement official responsible for implementing that statute. The Attorney General in turn delegated those responsibilities to the FBI. 28 C.F.R. § 0.85(o).

5. Over the last decade, the FBI has employed me as a consultant to address implementation issues raised by CALEA. The statute, among other things, requires that the equipment and services of telecommunications carriers, including wireless carriers, be capable of expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to intercept call content and call-identifying information. CALEA defines "call-identifying information" as "dialing or signaling information that identifies the origin, direction, destination, or termination of" a telephone call. See 47 U.S.C. § 1002(a) (paraphrased) and § 1001(2) (quoted).

6. Implementing such provisions required the telecommunications industry to develop technical standards in consultation with the FBI that meet the interception needs of law enforcement without unduly burdening the industry. A standard for the wireless telephone industry has been memorialized by the industry in a technical specification called "ANSI/J-STD-025A" commonly referred to as the "J-Standard."³ The J-Standard establishes industry benchmarks for compliance with CALEA,

[b4 b7E]

³ The most current version of the copyrighted J-Standard is entitled "ANSI/J-STD-025A - Lawfully Authorized Electronic Surveillance, April 2003." "ANSI" refers to the American National Standards Institute. Relevant excerpts of the J-Standard are attached hereto as Exhibit 1.

[b4 b7E]
[b4 b7E]

7. As a consultant to the FBI, I participated and continue to participate in the FBI's discussions with the telecommunications industry about law enforcement's electronic surveillance needs concerning wireless and wireline telephones. Through my experience as a network engineer and my participation in discussions with the telecommunication industry, I have a thorough understanding of the information resident in service providers' networks that is used for call processing or other business reasons (e.g., billing). I have been able to utilize this knowledge to assist the FBI in formulating contributions to the development of the J-Standard.

B. Basics Of Wireless Telephone Service

8. Providers of wireless telephone service in the United States generally use one of four radio frequency ("RF") formats to provide mobile cellular service: TDMA, CDMA, GSM and iDEN.⁴ Whichever of these formats it uses, a wireless carrier depends on location information to route calls to and from wireless telephones and to bill its customers. The following

⁴ TDMA stands for "Time Division Multiple Access" format; CDMA for "Code Division Multiple Access" format; GSM for "Global System for Mobile Communication;" and iDEN stands for "Integrated Digital Enhanced Network" format.

terminology describes basic functions within all four formats that support wireless telephone⁵ service:

9. **Wireless Telephones.** A wireless telephone is a low-power, mobile, two-way radio. It communicates with a carrier's wireless network over two, separate channels: a control channel, which carries data necessary to route and address calls to and from the wireless telephone and a content channel, which carries the contents of a call (e.g., voices). In response to a standard network signal, the wireless telephone periodically registers with the network by broadcasting a unique wireless ID. The wireless ID may include, for example, the telephone's serial number and assigned mobile telephone number.

10. **Cells, Cell-Sites, Towers and Sectors.** Every wireless carrier divides the geographic area served by its network (the wireless service area, or WSA) into numerous segments called cells. Conceptually, telecommunication engineers represent each cell as the union of three contiguous hexagons, each of which shares two bordering segments with the other (see diagram below). At the approximate center of each hexagon, the carrier maintains a cell-site antennae, or base station tower,

⁵ In this declaration, I use the term "wireless telephone" to refer not only to cellular telephones, or what is colloquially known as a "cellphone," but also to other mobile telephones, such as models that run on broadband PCS ("Personal Communications Services") networks, a digital radio frequency (RF) format that is widely used by the industry.

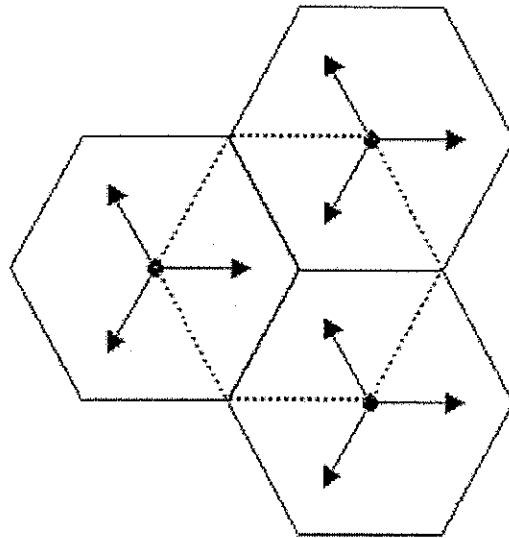
(tower). Every tower includes radio transmitting and receiving equipment and at least one antenna. Wireless carriers control the functions of multiple towers through the use of a base station controller, or base station.

11. A wireless telephone must be within radio range of a tower in order for the wireless telephone to make calls to or receive calls from the network. Each tower transmits and receives signals within a range of 360 degrees. A carrier typically divides that circular range into three equal slices of 120 degrees, each of which it designates as a sector of the tower. Sensors within the base station controller detect which tower and sector makes radio contact with a wireless telephone, thus providing a rough indication that the direction of the telephone lies within a 120-degree arc from the tower. Other sensors in the base station controller monitor the strength of the telephone's signal during the progress of the call.⁶ The fact that a wireless telephone is physically closer to a given tower does not necessarily mean that it uses that tower to contact the network. The radio frequency range of wireless telephones and base station towers is approximate and variable.

⁶ This information is used by the base station controller to manage the hand-off from one tower to another by comparing the strength of the telephone's radio signal relative to adjacent towers. Currently, the location information provided in accordance with the J-Standard does not disclose signal strength information, but rather, only tower and sector information recorded at the beginning and end of a call.

Impediments to transmission, e.g., large buildings or interference, can result in a wireless telephone having better signal strength to a tower other than the closest one.

12. The diagram below represents a cell, and within it, what is called a cell-site:⁷



The hexagons drawn in solid lines constitute the cell. The dots at the center of each hexagon are towers. Each arrow radiating from a tower represents a side, or face of that tower and its outward heading. Each face is assigned a 120-degree sector, represented by dotted lines. The hexagonal union of those dotted lines constitutes a cell-site.

⁷ Graphic From T. Farley and M. van der Hoek, Cellular Telephone Basics: AMPS and Beyond available on the Internet at <http://www.privateline.com/Cellbasics/Cellbasics.pdf>, at 11.

13. The size of a cell and thus, of a cell-site, is determined by, among other things, population density, topography, range of radio equipment and type of RF format. Depending on these factors, the radius of a cell could be as much as 30Km or as little as 200M (an approximate range of 18 miles to 656 feet).⁸ In general, the denser a WSA's population and/or development, the smaller the cells.

14. **Mobile Switching Centers.** Within every wireless network, the carrier assigns groups of cells (i.e., groups of towers and their respective base stations) to a mobile switching center (MSC). The MSC is the network's primary point of contact for receiving messages from or sending messages to a base station within any of the MSC's assigned cells. The MSC is a sophisticated computer that manages information addressed to and from wireless telephones in communication with all base stations in a WSA or all base stations in a WSA subregion (e.g., a large city or a state). The MSC's functions include:

- Capturing signals from its base stations conveying the wireless IDs of wireless telephones registering in the MSC's area, paired with data identifying the tower and sector (tower and sector information) with which each such telephone has registered;
- Verifying with a home location register (HLR)

⁸ The radius is the distance from the center of the hexagon to the intersection of two of its borders.

and/or visitor location register (VLR) that a wireless telephone seeking to register with the network is entitled to service. An HLR is a network's main database of subscriber information. A VLR is a database of wireless users "roaming" outside their home network(s) under reciprocal agreements with another network. A VLR communicates with the HLR of a reciprocating network to confirm that a roaming wireless telephone is entitled to reciprocity;

- Connecting calls between wireless telephones served by the same MSC and/or connecting calls to or from a wireless telephone in the MSC's area that are carried in part⁹ over a landline network (also known as a wireline network) or long distance carrier;
- Managing the hand-off from one base station to another of a call from or to a wireless telephone in motion. As a wireless telephone moves out of range of the tower(s) associated with a base station and into the range of another, the MSC controls the handover to ensure the continuity of a call in progress.¹⁰

C. Why and How Carriers Record
The SUBJECT TOWER/SECTOR & MSC RECORDS

15. The regulations implementing CALEA require that providers of wireless service expeditiously isolate and enable the government, pursuant to a court order or other lawful authorization, to access signaling information identifying towers

⁹ It is frequently the case that the content of calls to or from a wireless telephone travel in part over conventional wireline and/or long distance networks.

¹⁰ To manage the hand-off from one tower to another, the base station compares data reflecting the drop in strength of the telephone's radio signal to the first tower and rise in strength of the telephone's radio signal to the second tower.

and sectors used in the processing of calls to and from cellular telephones.¹¹ The J-Standard establishes an industry-wide protocol [b4 b7E]

[b4 b7E]

] See Exhibit 1 hereto.¹²

16. [b4 b7E]

[b4 b7E]

¹¹ See In the Matter of Communications Assistance for Law Enforcement Act, 14 F.C.C.R. 16794 (1999), upheld in relevant part, United States Telecom Ass'n v. FCC, 227 F.3d 450, 463-64 (2000).

¹² Exhibit 1 contains relevant excerpts of the copyrighted J-Standard. [b4]

(b4 b7E]
[b4 b7E]

17. In addition, as further explained below, service providers record the identity of the last-known MSC serving a telephone, as well as Locator Data at the beginning of a call, out of technological and billing necessity. Service providers also record Locator Data at the end of a call because this information is likely to prove useful in completing subsequent incoming calls (when registration with the network has not occurred in the interim) and is therefore efficient to record. Accordingly, carriers record last-known MSC, tower and sector information generated at the beginning and end of calls independent of any obligation imposed by CALEA or request by law enforcement and, when there is any such request, it is not complied with before the carriers have made those records for their own purposes.

18. **The Registration Process.** A wireless network must maintain approximate fixes on tens of thousands and sometimes hundreds of thousands of mobile, low-powered, wireless telephones in order to carry their calls. Meeting this goal depends on, among other things, the telephones registering with the network. Whenever a wireless telephone is switched on and detects a network control signal, it will register (or will attempt to register) with the network(s) in the WSA where the telephone is

located. Registration occurs whether or not that telephone makes or attempts to make a call and will periodically recur while a phone is powered on. Once a registering telephone's signal reaches a tower (the servicing tower), the base station (the servicing base station) sends to the MSC to which it is assigned (the servicing MSC) a message containing the wireless ID of that telephone, paired with codes identifying the tower and sector in contact with that telephone (the servicing tower and sector). The servicing MSC forwards this information (the Locator Data) to the HLR and/or VLR.

19. If the HLR confirms to the servicing MSC that the telephone is entitled to network service, the Locator Data, together with the identity of that MSC, is recorded on the HLR and/or VLR. That record remains in the HLR and/or VLR's memory unless and until the wireless telephone registers with a different tower and sector. When that happens, the updated information is conveyed to the servicing MSC, forwarded by it to

the HLR and/or VLR, recorded, displacing the old information -- and the cycle begins anew.¹³

¹³ As further discussed below, the displaced information is either purged from memory when the update is recorded or, in some networks, retained for other business purposes in a form that may be neither quickly nor easily accessible.

20. **Serving MSC Records.** If a wireless telephone travels from a region covered by one MSC to a region covered by another, that is, of course, important information for the network(s) involved. A network needs to know the identity of the MSC that is serving a telephone in order to continue to complete calls to or from it. Accordingly, when a wireless telephone moves into the region of a new MSC, the new serving MSC's identity is recorded in the HLR and/or VLR. This record is a form of location information, albeit a highly generalized one, since it does no more than identify the market served, which usually covers a large area, such as a major metropolitan area (e.g., New York City or Atlanta), of the kind that often appears in originating or terminating entries on a subscriber's bill.

21. **Location Data -- Beginning of an Outbound Call.** A wireless network relies on the Locator Data recorded on the HLR and/or VLR to complete calls from or to any wireless telephone in its WSA. In the case of an outbound call, a wireless telephone (the originating telephone) sends a message over the control channel requesting to place a call to another telephone (the terminating telephone). The message is picked up by the serving tower, which relays it, via the serving base station, to the serving MSC. The serving MSC (re)verifies with the HLR the caller's right to service and, if there has been a change in towers used by the caller since the last registration, updates

the Locator Data recorded at the HLR and/or VLR. The Locator Data thus recorded in the network's memory makes up tower/sector information for the beginning of an outbound call. This information constitutes the location information provided to law enforcement in an origination message specified in the J-Standard.

22. If the terminating telephone (or its surrogate, e.g., a voicemail service), does not pick up, the originating tower/sector remains in the memory of the HLR and/or VLR's until displaced as described above. If the terminating telephone answers, an answer signal is sent back across the network(s) to the serving MSC. The serving MSC reacts by directing the originating tower to open a content channel so the parties to the call can begin communicating. Thus, the network depends on its record of originating tower/sector information for the beginning of the call not only to locate the originating wireless telephone but also to connect it to the party that it called. Moreover, each network that maintains a reciprocal arrangement with others depends on the other networks to maintain records of such originating tower/sector information so that customers can make calls from their wireless telephones even when they are "roaming" outside their network.

23. **Location Data -- Beginning (Answer) of an Inbound Call.** Wireless networks are similarly dependent on

recorded Locator Data to complete inbound calls to a wireless telephone operating in its WSA. The network that serves the wireless telephone for which there is an inbound call routes the call to an MSC. That MSC contacts the HLR on which Locator Data for the wireless telephone is stored. The HLR confirms the identity of the tower last known to be serving the telephone, either by checking its own records or (if the telephone is roaming) the records of a VLR. Next, the MSC serving the telephone¹⁴ confirms and/or updates the Locator Data for that telephone in the HLR (or VLR). The Locator Data now recorded in the network's memory makes up tower/sector information at the beginning of an inbound call. [b4]

[b4]

24. The serving MSC thereupon uses that same information to page the telephone to which the inbound call is addressed. If the telephone (or its surrogate), does not pick up, the tower/sector information remains in the memory of the HLR and/or VLR until displaced when the telephone re-registers and/or places or receives another call. If the telephone answers, a signal confirming that it has done so is sent, via the serving base station, to its serving MSC. That MSC responds by directing

¹⁴ If the originating and terminating telephones are in cells served by the same MSC, there is only one MSC involved in this process.

the tower to open a content channel so that the parties to the call can begin communicating. Accordingly, each wireless network depends on its records of tower/sector information at the beginning of an inbound call to locate wireless telephones and connect them. Moreover, each network that maintains a reciprocal arrangement with others depends on the other networks to maintain records of such information so that customers can receive calls at their wireless telephones even when they are "roaming."¹⁵

25. **Location Data -- End of a Call.** Wireless networks also record on their HLRs and VLRs the last tower and sector that a wireless telephone used during a call. Carriers have long recorded and continue to record this information for several reasons. First, it enables the network to quickly reallocate resources that had been reserved to carry the call. When a user of a wireless telephone hangs up, he sends a message over the control channel informing the MSC that he has released the call. The MSC thereupon signals the serving tower to close the content

¹⁵ The foregoing summary of how wireless networks keep Locator Data in memory in order to, among other things, open content channels to complete incoming and outbound calls describes how the wireless industry has organized its networks for many years. In an earlier era, carriers used systems in which every time there was an inbound call, the MSC paged every cell-site and radio channel in order to find the telephone for which there was an inbound call. Systems of this kind were abandoned as inefficient, resource-intensive and tending to delay call completion. Accordingly, they have no bearing on how serving MSC and tower/sector information is recorded by the present-day industry.

channel to the telephone, thereby freeing content resources (e.g., tower frequencies) so that they are available to service other calls. Second, storing Locator Data at the end of a call gives the carrier a point of reference for the next call to or from the wireless telephone in question. Unless and until that telephone re-registers with the network, there is no need to expend resources updating Locator Data records. Third, a carrier may record the last as well as the first towers and sectors used during calls to create a database of cell-site usage patterns in a given WSA. The business rationales motivating many carriers to build these databases include marketing analysis, equipment usage and equipment upgrade studies and fraud management.¹⁶ [b4]

[b4]
[b4]
[b4]
c. [b7E]
26. [b4 b7E]
[b4 b7E]

¹⁶ In addition to these reasons, carriers historically billed for cellular usage on a per call basis and hence it was necessary to keep records of the last as well as the first tower for billing purposes. Cellular billing, at that time, was modeled on the local versus long distance billing model. Since the emergence of rate-plans that cover large home-areas and in some cases provide nation-wide coverage, carriers now generally track and bill based on airtime usage rather than distance.

[b4 b7E]
 [b4 b7E]
 [b4 b7E]
 [b4 b7E]

27. In general, a carrier needs to be aware of a particular subscriber's location when its network is supporting a call from or to that subscriber i.e., throughout the duration of the call. Accordingly, some carriers do not dedicate facilities for more than transient storage of Locator Data. Rather, storage of these records occurs as in the cycle previously described,

¹⁷ Carriers also record Locator Data for calls in progress. When a wireless call is carried by at least one other tower/sector in-between its beginning and end, the network detects the use of the interim tower(s)/sector(s) and stores the identity of the interim tower(s)/sector(s) on the HLR or VLR. []

[b4 b7E]
 []

with the most current tower and sector information for a telephone displacing the old. Thus, at the end of an hour in which a wireless telephone made or received five calls, the only tower/sector information that resides in an HLR or VLR as a result of attempted or completed calls is the tower and sector that was used at the end of the last call.

28. As mentioned above, other carriers do maintain databases of historical records, including tower and sector usage, with which to analyze market usage, equipment use or fraud patterns. But these databases compile data on millions of daily transactions and are designed to aggregate and summarize large-scale trends. As a result, law enforcement that makes an authorized request for such historical information encounters one of two poor outcomes. First, there may be no information available if the carrier does not maintain such a database. Second, even if there is a database, there will be significant delay in retrieving the requested information, owing to administrative obstacles (e.g., time passes before the carrier processes the request, conducts the search to extract the data, and forwards the results to law enforcement).

29. Under existing industry practice, standards and regulations, an authorized LEA can be best assured that it will receive all the tower/sector records that it has been empowered to obtain if the carrier isolates them soon after they are stored

on the HLR (or VLR) and then accessed by and copied to the IAP for collection by LEA. That is precisely what happens when a carrier complies with an order directing the disclosure of tower/sector information at the beginning and end of a call. As would occur regardless of whether an order is in place, the origination or termination of a call -- including the network's recording of Locator Data -- takes no more than a tenth of a second. Thereafter, the Locator Data is accessed by and copied to the network's IAP and, within the 8 seconds required by the J-Standard, the copied information is sent from the IAP to the LEA's collection point. In every instance, only after the tower/sector information has been recorded on the network for its own system purposes is a copy delivered to law enforcement.

D. What The Requested Tower/
Sector Records Are Not

30. The telecommunications industry has rapidly developed and marketed technologies that generate precise location information potentially subject to court-ordered electronic surveillance. Location-based services (LBS), for example, provide wireless subscribers personalized services tailored to their current location. LBS offer a new market for application developers and wireless network operators to develop and deploy value-added services: advising subscribers of current traffic conditions; supplying turn-by-turn navigation information; helping subscribers find nearby ATMs, restaurants, gas

stations, or any other location that can be found in the Yellow Pages. Other applications include fleet management or asset tracking -- allowing businesses to know the whereabouts of a vehicle, inventory, or even a salesperson/service technician; parents can use location-based services to monitor the location of children; and location-based gaming. A location application would necessarily interact with other location technology components to utilize the subscriber's location to provide a list of locations within a certain proximity to the mobile subscriber. In some instances, wireless carriers resell location information to third parties to make services available (e.g., aggregate subscriber location information used to generate real-time traffic reports).

31. **Method of Determining Location:** The method of determining location that is used by providers offering LBS can be divided into two general categories: network-based and handset-based.¹⁸ In general, network-based methods rely on

¹⁸ [b4 b7E] J-STD-036, a standard published by the Alliance for Telecommunications Industry Solutions, is the industry standard developed in response to the FCC E-911 mandate. See also 47 C.F.R. §§ 20.18(e), (g)(1)(v), (h), describing the FCC E-911 mandate which formed the basis for these parameters. A list of the FCC's E-911 wireless decisions is available at <http://www.fcc.gov/911/enhanced/release.htm#ro>. TIA-881, a standard published in 2004 "enable[s] a wireless

signals transmitted from the handset to the network during registration and/or call processing that enable the network to measure location. In handset-based methods, the subscriber's handset has a capability (e.g., because it contains a GPS-enabled computer chip), to provide location information when prompted by the network. As described below, each of these location methods materially differs from the tower/sector and MSC information that an authorized LEA obtains from a provider's IAP.

32. **Network-based Method.** There are three variations of the network-based method: time difference of arrival, time of arrival, and the angle of arrival. Each of these methods measures the radio frequency signals that are being transmitted between the handset and at least one tower receiving the signal. One of the simplest network-based methods, time difference of arrival, calculates location based on the time it takes for a subscriber's radio signal to travel from the handset to a tower. A minimum of three towers simultaneously receiving a signal from a handset are necessary for the network to be able to triangulate the position of the subscriber. To achieve accurate positioning, the location of the towers must be precisely known and the receiving equipment synchronized in time. This is similar to the function that the base station controller performs in the course

system to provide enhanced location services." See "TIA Publishes New Standard TIA-881," at http://www.tiaonline.org/media/press_release/index.cfm?parelease=04-65.

of a handoff when it compares the signal from the phone and the serving tower to the phone's signals to adjacent towers to determine whether to transfer service for that phone from one tower to another. To provide LBS to the phone, the network uses the same signal information it uses to effect hand-off during call-processing, but obtains a more precise calculation of the phone's position because it more precisely measures the signals.

33. The time of arrival technique is very similar to the time difference of arrival described above. The time of arrival technique uses the absolute time of arrival at a tower rather than the time difference between towers. Radio signals travel at a known velocity. So long as the precise location of a tower in communication with a phone is also known and the receiving equipment is synchronized in time, the tower's distance from the phone can be ascertained by multiplying the known velocity and the time elapsed between transmission from the telephone and arrival at the tower. This method, like the time difference of arrival method, measures the same radio signal that is transmitted from the phone to the tower to register with the network and to otherwise maintain service with the network.

34. The angle of arrival method uses multiple antennas at a tower to determine the angle of an arriving signal. If a handset is within line-of-sight, the receiving antenna can determine the direction from which the signal is coming. The

network compares similar data from a second tower to pinpoint the caller's location. Angle of arrival systems are designed to adjust for multi-path radio signals (signals that bounce off other objects), since they may confuse the location of the handset. Each of the above three methods measure radio signals from a phone that are otherwise received by the network and used in the provision of traditional cellular service.

35. **Global Positioning System (GPS) Method.** GPS-enabled handsets use signals from orbiting satellites to fix their respective positions. This location information is then transmitted from the handset to the network. In the past, the cost of GPS components in the handset made this a less desirable option, but prices have decreased enough to make even lower-end handsets GPS-enabled. Despite its accuracy, however, GPS may take a relatively long time (sometimes a minute or more) to obtain an initial fix on the location of a handset. To reduce this delay, the wireless industry developed "assisted GPS" (aGPS). In aGPS, the handset gets a head start by using its position relative to cell-sites that have known GPS coordinates to create an envelope of possible locations. This allows for the calculation of the handset's location to occur more quickly because fewer satellite signals need to be acquired. The network also provides the handset information for the specific satellite signals received by the handset to further reduce the time

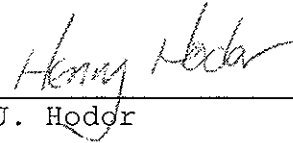
necessary to calculate location.

36. Tower/sector and MSC information disclosed consistent with the J-Standard does not yield the geographic precision that carriers require in order to provide location-based services, be they reliant on information generated by the network or in part provided by the handset. As a threshold matter, even if a network offers location-based services or a wireless telephone using that network is GPS-enabled, a carrier served with a court order or other legal authorization to provide tower/sector information will provide only the Locator Data recorded on a HLR or VLR in the ordinary course of tower-facilitated call service, not data computed based on time difference of arrival, time of arrival, or the angle of arrival, or GPS data.

37. Moreover, as previously explained, tower/sector information establishes only the general vicinity of a wireless telephone. For example, if a telephone is in a cell-site whose radius is 10 miles and transmits to one of its sectors, those facts would establish only that the telephone is somewhere within approximately 104 square miles, for that is the area covered by the sector. Even if a telephone is in a cell-site whose radius is 1 mile and transmits to one of its sectors, those facts would establish only that the telephone is somewhere within approximately 1.04 square miles. In addition, the above calculations

assume ideal equipment configurations and conditions and vary further depending on other factors, including whether the signals in the vicinity in which a subscriber is operating have been enhanced by third parties (e.g., in buildings whose management has installed amplifiers or directional antennae) or are impeded by topography. Actual tower/sector coverage areas are unique and customized to serve the population in a given geographic region.

I declare under penalty of perjury that the foregoing is true and correct. Executed pursuant to Title 28, United States Code, Section 1746 at Chantilly, Virginia, on this 23rd day of February, 2006.



Henry J. Hodor