Electronically Filed 03/26/2013 01:01:50 PM ET

RECEIVED, 3/26/2013 13:03:32, Thomas D. Hall, Clerk, Supreme Court

IN THE SUPREME COURT OF FLORIDA

SHAWN ALVIN TRACEY,

Petitioner,

v.

STATE OF FLORIDA,

Respondent.

Case No. SC11-2254

ON DISCRETIONARY REVIEW FROM THE
THE DISTRICT COURT OF APPEAL,
FOURTH DISTRICT OF FLORIDA

ANSWER BRIEF OF RESPONDENT

PAMELA JO BONDI
ATTORNEY GENERAL

CELIA TERENZIO
CHIEF ASSISTANT ATTORNEY GENERAL
Fla. Bar No. 656879

MELYNDA L. MELEAR
ASSISTANT ATTORNEY GENERAL
Fla. Bar No. 765570

Office of the Attorney General
1515 North Flagler Drive
Suite 900
West Palm Beach, FL 33401
Primary E-Mail:
CrimAppWPB@myfloridalegal.com
(561) 837-5000
(561) 837-5108(Fax)

COUNSEL FOR RESPONDENT

TABLE OF CONTENTS

TABLE OF CITATIONS

Cases

Florida Statutes

Federal Statutes

Miscellaneous

PRELIMINARY STATEMENT

This brief will refer to Petitioner as such, Defendant, or by proper name, e.g., "Tracey." Respondent, the State of Florida, was the prosecution below; the brief will refer to Respondent as such, the prosecution, or the State. The following are examples of other references:

IB = Petitioner's Initial Brief

R = Record on Appeal, volume followed by page

T = Transcripts on Appeal, volume followed by page

Unless the contrary is indicated, bold-typeface emphasis is supplied; cases cited in the text of this brief and not within quotations are underlined; other emphases are contained within the original quotations.

STATEMENT OF THE CASE AND FACTS

Respondent generally agrees with Petitioner's Statement of the Case and Facts, but makes the following clarifications and additions:

1. The application for an order authorizing the installation and use of a pen register/trap and trace device introduced the affiant as a law enforcement officer for nine years currently assigned to the Major Narcotics Unit of the Sheriff's Office (R1, 67). It certified that the requested installation was relevant to an ongoing investigation of illegal narcotics activities (R1, 67). It stated that a DEA confidential source indicated that Petitioner obtains multiple kilograms of cocaine from Broward County for distribution on the West Coast of Florida (R1, 68). It also asserted that the confidential source contacts Petitioner on the listed Metro PCS number (R1, 68).

2. The order, entered on October 23, 2007, authorizing the installation of a pen register/trap and trace device directed:

> In accordance with US Title 18, Section 2703(d), it is further Ordered that, Metro PCS their agents and /or the appropriate providers of the wire and/or electronic communications services shall furnish the Broward County Sheriff's Office with historical Cell Site Information indicating the physical locations of the cell sites, along with cell site sectors, utilized for the calls so long as the telephone numbers(s)/facilities, cable or pair and/or electronic serial number remain the same.

(R1, 73).

3. At the hearing on the motion to suppress, Petitioner testified that he acquired and purchased a Metro PCS cell phone with number (***) ***-2470 (T3, 16-19). He used the name "Chris Barron," which he made up, used a different date of birth, and listed his old address on the application for the cell phone (T3, 20-24). He said, "The whole name, the whole setup is not accurate" (T3, 24).

4. Detective Jason Hendrick testified at the hearing that for the investigation, the Sheriff's office had one building, the tech support headquarters, where a detective monitored "a computer that was receiving the data from Metro PCS, and he was able to tell you through the cell site information where Mr. Tracey's car was progressing" (T3, 51). Detective Hendrick explained how law enforcement ultimately located Petitioner's vehicle:

> Well, it's not like, you know, Sergeant Cunneen calls and says, hey, they're at this address and then we went there. You have to understand that -- that the surveillance we had set up at different locations as Mr. Tracey bypassed those locations, a light went off, hey, he's not going to that, and so we readjusted. And we basically mirrored and shadowed him until we were in that area as well.

(T3, 52).

He pointed out that law enforcement also had a trap and trace on the person Petitioner was meeting, "Vilbon" (T3, 53). He said, "We were able to see that both phones were inside that location [the Miramar address]"(T3, 53). He said that they saw

two cars there, one a GMC Envoy with tags that came back to a Cape Coral address (T3, 54). The other vehicle had a temp tag for the East Coast (T3, 54). He testified that law enforcement had originally been staking out places associated with Vilbon, one in Pompano and one in Miramar (T3, 63).

4. Sergeant Bill Cunneen testified that law enforcement had two addresses for Vilbon in Broward County, one in Pompano and one in Miramar (T3, 68). The Miramar address was a few blocks away, less than a mile, from where Vilbon actually was that night (T3, 70). He stated that the traffic out near the stash house was minimal, at between 1:30 and 2:00 in the morning (T3, 71).

Sergeant Cunneen said that he had been at the main office to get cell site information on Petitioner's and Vilbon's phones (T3, 73). He stated:

> Basically I get – there was a number coming up for a cell site that corresponded to – it was a Metro PCS cell phone that corresponded to – they have an Excel spreadsheet which has the cell site number and then the address for that cell site, so from the cell site number I was able to get an address of where that cell site was located.

(T3, 73).

He said that kept changing over the course of the evening (T3, 386).

Sergeant Cunneen said that he got into his vehicle and headed to Miramar when he saw that Petitioner's phone was in the area of East Broward by US 1 and 595 "[b]ecause Mr. Vilbon's phone,

the cell site information that we had on that phone, it remained down in the Hollywood/Miramar area" (T3, 74).

Sergeant Cunneen explained that the cell site information for Metro PCS provides a location address for the particular cell site number (T3, 79). It also provides a number that indicates the section of the tower receiving the signal so that the direction can be determined, for instance northwest, southeast, etc. (T3, 80). He stated that they only received the cell site information when the phones were actually being used (T3, 82). He explained that a "dormant" phone would not transmit a "ping" of a particular cell tower (T3, 83).

5. Special Agent Marco Moncayo of the Drug Enforcement Administration testified that he received information from an agent in New York that someone in Miami wanted to provide information (T3, 87). He said that he met with this person in July of '07 and this person provided him with information that Petitioner had made trips to Broward to pick up drugs on a number of occasions and that Petitioner was incarcerated at the time (T3, 87). He said that he provided this information to the Broward Sheriff's Department and that they waited on Petitioner to be released (T3, 88). He stated that he received a call from the informant in December of '07 that Petitioner had reached out to him to run a trip to pick up drugs in Broward (T3, 401). He

monitored calls between the informant and Petitioner (T3, 88-89).

6. At trial, Sergeant Cunneen testified that both phones being watched were in the same general area (T4, 368). He said that there were at least three calls between the two phones once Petitioner started traveling to Broward (T4, 377).

SUMMARY OF ARGUMENT

The trial court properly denied the motion to suppress. The use of the cell-site location information did not violate the Fourth Amendment. Petitioner does not have a subjective or objective expectation of privacy in the cell phone data which he shared with the provider every time he dialed his cell phone or answered it. He does not have an objective expectation of privacy in his location outside of the home where he used the cell phone on the public highway where his movements could readily be viewed by any person along the route. The information did not even reveal Petitioner's precise location but only indicated the particular direction of the cell tower's address. The information provided by the cell provider in this case did not allow for readily calculating Petitioner's exact location. In addition, the information was not aggregated in any comprehensive or long-term manner.

Law enforcement provided specific statements in the application setting out a need, but even if the statements were not an adequate showing of relevancy, suppression is not a remedy for violation of the statute. Petitioner's location was revealed by an independent source, his co-perpetrator's cell phone "pings," and, in any case, would have been inevitably discovered. Law enforcement acted in good faith based on order authorizing the disclosure of historical CSLI.

ARGUMENT

THE TRIAL COURT PROPERLY DENIED THE MOTION TO SUPPRESS; THE USE OF THE CELL-SITE LOCATION INFORMATION DID NOT VIOLATE THE FOURTH AMENDENT.

Petitioner argues that the trial court erred in denying the motion to suppress because law enforcement should not have been permitted to obtain real-time Cell-Site Location Information (CSLI) from Petitioner's cell phone provider based on anything less than a showing of probable cause. Respondent disagrees and maintains that Petitioner's rights under the Fourth Amendment to the United States Constitution were not violated by the use of the information, and, therefore, the trial court properly denied the motion to suppress.

A. Standard of Review

The standard of review for orders on motions to suppress is to accord historical facts with a presumption of correctness but review *de novo* mixed questions of law and fact that ultimately determine constitutional issues. Welch v. State, 992 So. 2d 206, 214 (Fla. 2008).

B. Discussion of CSLI obtained in this case

Detective Jason Hendrick testified at the hearing that for the investigation, the Sheriff's office had one building, the tech support headquarters, where a detective monitored "a computer that was receiving the data from Metro PCS, and he was

able to tell you through the cell-site information where Mr. Tracey's car was progressing" (T3, 51). Sergeant Cunneen said that he had been at the main office to get cell-site information on Petitioner's and Vilbon's phones (T3, 73). He stated:

> Basically I get – there was a number coming up for a cell site that corresponded to – it was a Metro PCS cell phone that corresponded to – they have an Excel spreadsheet which has the cell site number and then the address for that cell site, so from the cell site number I was able to get an address of where that cell site was located.

(T3, 73).

He said that kept changing over the course of the evening (T3, 386).

Sergeant Cunneen explained that the cell site information for Metro PCS provides a location address for the particular cell site number (T3, 79). It also provides a number that indicates the section of the tower receiving the signal so that the direction can be determined, for instance northwest, southeast, etc. (T3, 80). When asked if each cell tower had three cones, Sergeant Cunneen said that they had two cell sites associated with them (T3, 79). He stated that they only received the cell-site information when the phones were actually being used (T3, 82). He explained that a "dormant" phone would not transmit a "ping" of a particular cell tower (T3, 83).

Based on the testimony, the State stresses three significant points about the CSLI in this case. First, law enforcement did not receive the cell tower "pinging" information directly from

the cell phone at the same time as Metro PCS. Rather, Metro PCS provided the information in a chart format to law enforcement after it first received the "ping." Second, Metro PCS, and, in turn, the Sheriff's Office, did not receive "pinging" or location information except when the cell phone was actually in use; location information was not received from a "dormant" state. Third, the location information obtained was for the location of the cell tower off which the cell phone "pinged," and not of the address where the phone was actually located.

C. The use of CSLI in this case did not constitute a search under the Fourth Amendment.

1. Petitioner's subjective expectation of privacy in CSLI

At the hearing on the motion to suppress, Petitioner testified that he acquired and purchased a Metro PCS cell phone with number (***) ***-2470 (T3, 16-19). He used the name "Chris Barron," which he made up, used a different date of birth, and listed his old address on the application for the cell phone (T3, 20-24). He said, "The whole name, the whole setup is not accurate" (T3, 24).

In order to determine whether a Fourth Amendment search has occurred, the court must determine whether the individual manifested a subjective expectation of privacy in the item or placed searched and consider whether society is willing to recognize this expectation as reasonable. Kyllo v. United States, 533 U.S. 27, 33, 121 S.Ct. 2038, 150 L.Ed2d 94 (2001).

The subjective aspect requires that the person shows an actual expectation of privacy. Minnesota v. Carter, 525 U.S. 83, 88, 119 S.Ct. 469, 142 L.Ed 2d 373 (1998).

The State asserts that Petitioner did not have a subjective expectation of privacy in the cell phone. He kept the phone under a completely made-up persona. This act suggests that Petitioner was trying to distance himself from the use of the cell phone. See United States v. Suarez-Blanca, 2008 WL 4200156 *7 (N.D. Ga. Apr. 21, 2008). One court noted that law enforcement has encountered a problem with persons obtaining cell phones in false names to avoid law enforcement detection by way of cell phone company records. See United States v. Madison, 2012 WL 3095357 *8 (S.D. Fla. July 30, 2012).

2 Objective expectation of privacy in CSLI as data

Regardless of whether Petitioner had a subjective expectation of privacy in the use of the cell phone, any expectation of privacy in the data generated and maintained as a result of its use is not reasonable by societal standards. The CSLI in this case is akin to historical cell site location information. Indeed, in United States v. Jones, 2012 WL 6443136 *3 (D.D.C. Dec. 14, 2012), the District Court recognized:

> Cell-site records may be obtained from the cell phone companies in two ways. The government may obtain this information after the fact, by requesting all such data accumulated over a specified time period. This is known as "historical" cell-site data. Alternatively, the government

> may seek to obtain this information on a real-time basis going forward from the date of the magistrate judge's order. This is known as "prospective" cell-stie data. **The information is "identical regardless of whether it is obtained historically or prospectively."**

(emphasis supplied)

First, the information in this case was generated, recorded and relayed only when Petitioner used his phone. The information was not obtained when the phone was not being used or was "dormant." When calls are made cell phones communicate with a particular cell-site tower that corresponds with the location where the call was made. United States v. Hardrick, 2012 WL 4883666 *3(E.D. La. Oct. 15, 2012). Cell phone providers maintain records listing the cell-sites that users' phones have communicated with and the times of the communications. Id. This information is retained and often appears on a users' bill. In the Matter of an Application of the United States for an Order Authorizing Disclosure of Location information of a Specified Wireless Telephone, 849 F. Supp. 2d 526, 534 (D. Md. 2011). On the other hand, while many cell phones today now routinely collect location information at various time-intervals when the phone is not in use, many providers only retain such "registration data" for ten minutes or so. Id.[1]

[1] Again, the Sheriff's Office did not receive such information. There was no discussion at the hearing on Metro

In circumstances like those in the present case, one District Court analogized a cell tower to a communication company's switching equipment that allows the call to proceed. United States v. Madison, 2012 WL 3095357 *8(S.D. Fla. July 30, 2012). It reasoned that in order for a cellular connection to occur, a user's cell phone must transmit to a cell tower within range. Id. It noted that most users are aware that when they are outside of the range of cell towers, a call cannot be connected or will be dropped. Id. It also pointed out that cell phone users know that their providers make and maintain permanent records of their phone usage for billing purposes. Id. It determined, therefore, that the defendant in the case before it knowingly and voluntarily gave information to his communications-service provider that he was located within a certain range of specific cell towers when he placed calls and received calls on his phone. Id. at *9.

In United States v. Suarez-Blanca, 2008 WL 4200156 *9 (N.D. Ga. April 21, 2008), the Magistrate Judge made a similar determination. The Magistrate Judge found little difference between CSI and other business records held in the course of business, like those of banks and utilities. 2008 WL 4200159 at

---

PCS' practices with regard to "registration" data. The State points out that the cell site information was obtained in 2007.

*9. In fact, many cases hold that the government may obtain historical cell site location information without a showing of probable cause because users do not have a reasonable expectation of privacy in such data. See, e.g., In the Matter of the Application of the United States of America For an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government, 620 F. 3d 304 (6th Cir. 2010); United States v. Ruby, 2013 544888 *6 (S.D. Feb. 12, 2013); In the Matter of the Application of the United States of America For and Order Pursuant to Title 18, United States Code, Section 2703(d) to Disclose Subscriber Information and Cell Site Information, 849 F. Supp. 2d 177 (D. Mass. 2012); U.S. v. Graham 846 F. Supp. 2d 284 (D. Md. 2012); United States v. Dye, 2011 WL 1595255 *9 (N.D. Ohio Apr. 27, 2011); United States v. Benford, 2010 WL 1266507 (N.D. Ind. Mar. 26, 2010); United States v. Suarez-Blanca, 2008 WL 4200156 (N.D. Ga. Apr. 21, 2008); In re Application of the United states of America for Orders pursuant to Title 18, United States Code, Section 2703(d), 509 F. Supp. 2d 76, 80 (D. Mass. 2007); People v. Hall, 86 A.D. 3d 450 (N.Y. App. 2011); Mitchell v. State, 25 So. 3d 632 (Fla. 4th DCA 2010).

The rationale behind these holdings is in part based on the principle that matters voluntarily shared with third-parties are not clothed in an expectation of privacy. In United States v.

Miller, 425 U.S. 435, 96 S.Ct. 1619, 48 L.Ed. 2d 71 (1976), the United States Supreme Court held that there was no Fourth Amendment intrusion when the government subpoenaed bank records from two banks that consisted of checks and deposit slips of the respondent. 425 U.S. at 440. The Court stated that the records were not the personal papers of the respondent, but, instead, were business records of the bank. Id. It noted that all of the documents obtained, including financial statements, contained only information voluntarily conveyed to the banks and exposed to the banks' employees in the ordinary course of business. Id. at 442. It concluded that the depositor takes the risk, in revealing his affairs to another, that the information will be conveyed to the government. Id. at 443.

Later, in Smith v. Maryland, 442 U.S. 735, 99 S.Ct. 2577, 61 L.ed 2d 220 (1979), the Supreme Court applied this rationale to dialed phone numbers. The Government in Smith requested that the phone company install a pen register on the petitioner's phone. The pen register records all numbers dialed on the line for which it is installed. 442 U.S. 736 n. 1. In considering the phone user's expectation of privacy, the Court noted that all telephone users realize that they must "convey" phone numbers to the telephone company, since it is through telephone-company switching equipment that calls are completed. Id. at 742. It stated that electronic devices like pen registers are

actually used by the phone companies to keep billing records of toll calls. Id. Hence, the Court concluded that even if the petitioner had some subjective expectation of privacy, it would not be an expectation that society is prepared to recognize as reasonable since a person has no legitimate expectation of privacy in information that he voluntarily provides to a third party. Id. at 743-744.

The State maintains that in an extension of the reasoning set out in Smith, Petitioner did not have a legitimate expectation of privacy in the data generated and maintained by the cell phone company as to the cell towers which his cell phone "pinged" because he voluntarily gave this information to the cell phone company when he dialed his phone or answered his calls. In In re Application of the United States of America for an Order Pursuant to 18 U.S.C. S. 2703(d), 830 F. Supp. 2d 114, 136 (E.D. Va. 2011), on an order directing Twitter to provide the Government with IP address information of subscribers, the court noted:

> The fact that a particular user may not see or know which IP address he is using at a particular moment does not create a reasonable expectation of privacy in the information. If the user is communicating over the Internet, intermediary computers and the destination computer must know the IP address as a condition of communication. Under the Fourth Amendment, that fact renders unreasonable any expectation of privacy in the IP address.

3. Objective expectation of privacy in the CSLI

While courts considering the acquisition of CSLI often focus on the business record aspect of the data maintained by the cell phone companies, courts considering the acquisition of real-time cell site information focus on the location information that the cell phone user has willingly exposed to others by virtue of where the user communicates on the phone, as well as by the type of location information that is provided by the cell phone company.

In United States v. Forest, 355 F. 3d 942 (6th Cir. 2004), vacated on other grounds, Garner v. United States, 543 U.S. 1100, 125 S.Ct. 1050, 160 L.Ed.2d 1001 (2005), a case involving a Drug Enforcement Agent dialing the defendant's number several times a day to use computer data to determine which cellular towers were hit, the Sixth Circuit concluded that the defendant had no expectation of privacy in the cell-site location information because the agent could have obtained the same information by following the defendant's vehicle. 355 F. 3d at 950-951. The court relied on United States v. Knotts 460 U.S. 276, 103 S.Ct. 1081, 75 L.Ed.2d 55 (1983) in support of its conclusion. Id.

In Knotts, the court considered whether law enforcement's tracing of signals from a beeper, a radio transmitter that emits periodic signals that can be picked up by a radio receiver,

violated the defendant's Fourth Amendment rights The beeper had been placed in a five gallon drum purchased by a co-defendant,. The Supreme Court stated that the governmental surveillance amounted to the following of an automobile on public streets and highways. Id. at 281. It concluded that visual surveillance from public places along the route of the defendant's travels would have revealed the same facts to the police. Id. at 282. It ruled that nothing in the Fourth Amendment prohibited the police from augmenting their sensory faculties with enhancement that technology afforded them. Id.

In State v. Jones, 22 A.3d 114 (N.J. App. 2011), the court applied the reasoning of Knotts to the police having obtained cell phone registration data, T-Mobile's scanning every seven seconds for the strongest signal of the nearest tower. 22 A. 3d at 117-118. The court concluded that the use of the information concerning the defendant's "general location" did not violate any expectation of privacy that the defendant may have had with regard to the location of his vehicle. Id. at 123. Citing to Knotts, the court determined that the defendant conveyed to anyone who wanted to look, the fact that he was traveling over particular roads in a particular direction and ended at a particular destination. Id. at 124. See also Devega v. State, 689 S.E.2d 293, 299-300 (Ga. 2010)(counsel not ineffective for failing to move to suppress evidence derived from real-time

cell-site information because no Fourth Amendment violation in use of "ping" information to track movement).

The State recognizes that the year after Knotts was decided, the Supreme Court held in United States v. Karo, 468 U.S. 705, 104 S.Ct. 3296, 82 L.Ed2d 530 (1984) that the transfer of a container secretly containing a beeper was a search because the beeper was used to learn information about a private residence. The transfer of the container was by a government informant who sold ether to the respondent to extract cocaine from clothing, and the intrusion occurred because the container remained in a residence for an extended period of time.

The instant case, however, is distinguishable from Karo. First, in this case, the CSLI obtained was only with regard to Petitioner's travel on public roads like in Knotts. While law enforcement was alerted to the fact that Petitioner stopped at the "stash house," just as in Knotts, the police could have observed this stop by visual surveillance as anybody could have from the public street.

Second, in Karo, the beeper placed in the container of ether alerted law enforcement to a fact that the ether was delivered to the residence and stayed there. The Supreme Court observed in Karo:

> In this case, had a DEA agent thought it useful to enter the Taos residence to verify that the ether was actually in the house and had he done so surreptitiously and without a warrant, there is little doubt that he would have engaged

> in an unreasonable search within the meaning of the Fourth Amendment. For purposes of the Amendment, the result is the same where, without a warrant, the Government surreptitiously employs an electronic device to obtain information that it could not have obtained by observation from outside the curtilage of the house. The beeper tells the agent that a particular article is actually located at a particular time in the private residence and is in the possession of the person or persons whose residence is being watched. Even if visual surveillance has revealed that the article to which the beeper is attached has entered the house, the later monitoring not only verifies the officers' observations but also establishes that the article remains on the premises. Here, for example, the beeper was monitored for a significant period after the arrival of the ether in Taos and before the application for a warrant to search.

468 U.S. at 715.

The Court in Karo expressly noted that these facts distinguished the situation in Karo from the situation in Knotts. Id. Here, law enforcement did not learn anything from the cell tower "pings" other than the cell phone was in the general area of the tower near the "stash house" address. See Kyllo v. United States, 533 U.S. 27, 32, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001)(warrantless visual surveillance of a home is lawful).

The State points out that the information that the Government obtained in this case, that the cell phone was being used near a particular address, is no different than the type of information that the Government may obtain when it installs a pen register on a suspect's home phone. See In the Matter of the Application of the United States for an Order, 411 F. Supp. 2d 678, 682

(W.D. La. 2006). In such a scenario, the suspect's location is disclosed every time the suspect dials the phone. Id. The cell phone provides much less specific information because the suspect could be using the phone in the back yard or even down the street. Id.

Of course, in this case, the cell phone "pings" did not even reveal the exact address of the "stash house," but instead gave the address of the cell tower that was hit, thereby disclosing the general location of the house. See In re Application for an Order Authorizing the Extension and Use of a Pen Register Device, 2007 WL 397129 *2 n. 2 (E.D. Cal. 2007)(court noted that only monitoring of cell phone was done outside the home via cell towers). Sergeant Cunneen testified that law enforcement was only provided a list from Metro PCS that had the address of the cell tower and the section number of it (T3, 79-80). He also testified that each cell tower had two cell sites associated with it (T3, 79).

Hence, the testimony in this case suggests that law enforcement may not have been provided information needed to engage in triangulation to determine the actual location of the cell phone. In In re Application of the United States for an Order for Prospective Cell Site Location Information on a Certain Cellular Phone, 460 F. Supp.2d 448 (S.D.N.Y. 2006), the

District Court explained the process of triangulation as follows:

> The location of the antenna tower receiving a signal from a given cellular telephone at any given moment inherently fixes the general location of the phone. Indeed, in some instances, depending upon the characteristics of the particular network and its equipment and software, it is possible to determine not only the tower receiving a signal from a particular phone at any given moment, but also in which of the three 120-degree arcs of the 360-degree circle surrounding the tower the particular phone is located. In some cases, however, the available information is even more precise.
>
> Often, especially in urban and suburban areas, the signal transmitted by a cellular telephone is received by two or more antenna towers simultaneously. Knowledge of the locations of multiple towers receiving signals from a particular telephone at a given moment permits the determination, by simple mathematics, of the location of the telephone with a fair degree of precision through the long established process known as triangulation.[citation omitted]. Real time information concerning the location permits geographic movements of the phone to be tracked as they occur.

460 F. Supp. 2d at 451.

The court defined triangulation as the process of determining the coordinates of a point based on the known location of two other points. Id. at n. 3.

The court went on to explain, "Where the law enforcement agents obtain information from only one tower at a time, they can determine that a cell phone is in the cell served by the tower and, in some cases, which sector of the tower faces the cell phone; but they can neither pinpoint the precise location of the cell phone nor track its movements." Id. at 452. "While

cell-phone users do not technically convey their location, they do voluntarily convey their cell-phone signal to the cell towers, and expose that information to cell-phone service provider's equipment in the ordinary course of business." In the Matter of an Application of the United States of America for an Order Authorizing the Release of Historical Cell-Site Information, 809 F. Supp. 2d 113, 122 (2011).

4. Impact of United States v. Jones, __ U.S. __, 132 S.Ct. 945, 181 L.Ed. 2d 911 (2012) on privacy analysis

Respondent realizes that the concurrences in United States v. Jones, __ U.S. __, 132 S.Ct. 945, 181 L.Ed. 2d 911 (2012) make clear that situations involving the mere transmission of electronic signals without a physical trespass remain subject to expectation of privacy analysis. 132 S. Ct. at 955, (Justice Sotomayor, concurring) Justice Alito, joined by Justices Ginsburg, Breyer and Kagan, stated that he would analyze the question presented in Jones as to whether the respondent's reasonable expectations of privacy were violated by the "long-term monitoring of movements of the vehicle." Id. at 958.

A couple of facts distinguish this case from the type of long-term monitoring referred to by the concurring justices in Jones. For one, the CSLI in the instant case does not provide the precise details that GPS does. It only reveals a sector of a cell tower at a time, thereby limiting a location to a general

area, but not revealing an exact address of an institution frequented by someone who would rather keep such information confidential. In addition, there is no evidence of long-term monitoring; based on information from monitored calls with the confidential informant, law enforcement tracked Petitioner on a single trip across the state.

Justice Sotomayor in her concurrence did indicate that she would ask in all instances of electronic monitoring if people would reasonably expect that their movements would be recorded and aggregated in a manner that allows the Government to ascertain a person's beliefs and personal habits. Id. at 955-956. Justice Alito's concurrence, however, made clear that "relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable." Id. at 964. Justice Alito cited to Knotts in support of this statement. Id.

In Knotts, the Court specifically stated, "When Petschen travelled over the public streets he voluntarily conveyed to anyone who wanted to look the fact that he was travelling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property." 460 U.S. at 281-282. Thus, it is not just the revelation of where a person

goes or in what activities that person engages outside of the home that renders a legitimate expectation of privacy.

Justice Alito also recognized in Jones that advances in technology may lead to changes in the public's expectations. Id. at 962-963. He referenced the emergence of closed-circuit television video monitoring, devices on toll roads that record movements of motorists, and roadside assistance devices that allow central stations to ascertain a car's exact location. Id. at 963. Under a consideration of how technology assists law enforcement in readily conducting surveillance, the State makes the argument that society is even less likely than just a few years ago to deem reasonable an expectation of privacy in information that a cell phone user shares with a cell phone provider about a cell phone provider's towers.

For the most part, post-Jones, it appears that courts have zeroed in on the cumulative amount of information about a person that has been acquired in comprehensive tracking. In United States v. Skinner, 690 F. 3d 772 (6th Cir. 2012), the court distinguished the three-day tracking from the "extreme comprehensive tracking" of twenty-eight days in Jones. 690 F. 3d at 780. In United States v. Graham, 846 F. Supp. 384 (D. Md. 2012), the court referred to the concern about prolonged and precise surveillance as a new "mosaic" approach which looks at the aggregate of information. 846 F. Supp. at 391. The location

information in this case is neither prolonged nor precise. See United States v. Sereme, 2012 WL 1757702 (M.D. Fla. Mar. 27, 2012)(no Fourth Amendment violation where Government tracked for 12 days by cell phone GPS the defendant's movements). Moreover, the information obtained was limited at all times to the exterior location of Petitioner's vehicle, and was not about what Petitioner was doing inside any location, public or otherwise.

5. Discussion of Petitioner's assertions

Petitioner makes the assertion that a "clear majority" of federal courts have held that the production of real-time CSLI requires the government to establish the existence of probable cause (IB. 17). Respondent clarifies this assertion by providing context by way of the District Court's opinion in United States v. Jones, 2012 WL 6443136 *7(D.D.C. Dec. 14, 2012):

> As this discussion reveals, there is a robust debate over the question of whether the Fourth Amendment applies to cell-site data obtained from a cellular provider, but to date, this Court knows of no federal court that has held that the use of prospective cell-site records constitutes a search under the Fourth Amendment, or of any federal court that has suppressed any type of cell site data obtained pursuant to a court order under the SCA [footnote omitted].

The court then went on to explain by way of footnote that while some courts have concluded that the government must show probable cause, they have so found based on their interpretation of federal statutory schemes not authorizing disclosure on a

lesser showing. Jones, 2012 WL 6443136 at *7 n. 14. The court also noted in the opinion that a "majority" of courts have held that there is no reasonable expectation of privacy in historical CSLI. Id. at *5.

Petitioner cites to two cases in support of his contention about the state of federal law (IB. 17). In the Matter of the Application of the United States of America for an Order Directing the Provider of Electronic Communication Service to Disclose Records to the Government, 534 F. Supp. 2d 585 (W.D. Pa. 2008), vacated, 620 F. 3d 304 (3d Cir. 2010), the court declined to follow the many courts holding that real-time cell-site information could be obtained by applications for orders under a combination of two statutes, and, therefore, decided that a writ under the federal rules was required, but the Circuit Court later disagreed with this approach. In In the Matter of an Application of the United States of America for an Order Authorizing the Use of a Pen Register with Caller Identification Devise Cell Site Location Authority on a Cellular Telephone, 2009 WL 159187*6 (S.D.N.Y. 2009), the court similarly declined to stretch the language of the statutes and held that a solution for obtaining the CSLI was to proceed under Rule 41, Federal Rules of Criminal Procedure, by making a showing sufficient to obtain a warrant. It did not address the Fourth Amendment in any way.

Petitioner suggests that the acquisition of real-time CSLI in this case violated the right of privacy under Florida's Constitution (IB. 19). Not only did Petitioner fail to argue this in the motion to suppress, but in State v. Hume, 512 So. 2d 185, 188 (Fla. 1987), a case involving the simultaneous transmission of personal conversations in the defendant's home, this court concluded that the right to privacy under article I, section 23, of the Florida Constitution, does not modify the applicability of article I, section 12, of the Florida Constitution, on search and seizure.

D. Law enforcement set out facts needed to justify the order for CSLI.

1. Statutory standard for obtaining CSLI

Section 934.23(4)(a)(2), Florida Statutes (2007), provides that law enforcement may require a "provider of electronic communication service or remote computing service" to disclose a "record or other information pertaining to the subscriber or customer of such service, not including the contents of a communication," only when the officer obtains a court order for such disclosure under 934.23(5). In turn, section 934.23(5), Florida Statutes (2007), states that a court order under subsection (4) shall issue only if the law enforcement officer "offers specific and articulable grounds to believe" that "the records or other information sought are relevant and material to an ongoing investigation." "Electronic communication service"

means "any service which provides to users thereof the ability to send or receive wire or electronic communications." Section 934.02(15), Florida Statues (2007).

As noted by the Fourth District in this case, section 934.23(4)(a)(2) is similar to the Stored Communications Act, Title II of the Electronics Communications Privacy Act of 1986, 18 U.S.C. Sections 2701-2712. See Tracey v. State, 69 So. 3d 992, 997 (Fla. 4th DCA 2011). 18 U.S.C. Sections 2703(c)(1) and (d) use the same language of sections 934.23(4)(a)(2) and (5).

Federal courts have grappled over time as to what statutory authority law enforcement has to obtain CSLI. Most recognize that the actual capture of "signaling information," as referred to in the definition of "pen register" under 18 U.S.C. Section 3127(3), is through the installation of a pen register, but note that 47 U.S.C. Section 1002(a)(2) of the Communications Assistance for Law Enforcement Act of 1994, on the requirements for telecommunications providers to provide information to law enforcement, states that with regard to information acquired "solely pursuant to the authority of pen register and trap and trace devices" information shall not disclose the physical location of the subscriber. From the language "solely pursuant," courts have reasoned that the pen register statute may be combined with another mechanism to obtain CSLI. Many have determined that 18 U.S.C. Section 2703(d) is the other mechanism

since it refers to the disclosure of a record or other information pertaining to a subscriber of electronic communications service. See, e.g., In re the Matter of an Application of the United States of America for an Order Authorizing the Use of Two Pen Register and Trap and Trace Devices, 632 F. Supp. 2d 202 (E.D.N.Y. 2008); In re Applications of the United States for Orders Pursuant to Title 18 U.S.C. Section 2703(d), 509 F. Supp. 2d 82 (D. Mass. 2007); In re Application of the United States of America for an Order for Disclosure of Telecommunications Records and Authorizing the Use of a Pen Register and Trap and Trace, 405 F. Supp. 2d 435 (2005); In re Application for Pen Register an Trap and Trace Device with Cell Site Location Auth., 396 F.Supp. 2d 747 (S.D. Tex. 2005). See also In the Matter of the Application of the United States of America for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government, 620 F. 3d 304 (3d Cir. 2010); United States v. Madison, 2012 WL 3095357 (S.D. Fla. July 30, 2012).

The courts' reasoning would apply to section 934.23(4)(a) because of the similarities in language. The Fourth District in this case pointed out, citing to State v. Rivers, 660 So. 2d 1360, 1362 (Fla. 1995), that at least with regard to the federal wiretap statute, this Court has found that the federal legislation preempted the field of interception of wire

communications. Tracey, 69 So. 3d at 998. It makes sense, then, that this court would seek guidance of federal interpretations of the scope of the federal law on electronic communications and find that CSLI may be obtained pursuant to an order obtained by way of section 934.23(5). See United States v. Sereme, 2012 WL 1757702 (M.D. Fla. Mar. 27, 2012)(court found no Fourth Amendment violation where Government tracked defendant's movements by GPS on his cell, in accordance with section 934.32, 12 days).

2. Showing in this Case

Respondent makes the argument that law enforcement made a showing of "specific and articulable grounds to believe" that "the records or other information sought are relevant and material to an ongoing investigation," pursuant to section 934.23(5). The application for an order authorizing the installation and use of a pen register/trap and trace device introduced the affiant as a law enforcement officer for nine years currently assigned to the Major Narcotics Unit of the Sheriff's Office (R1, 67). It certified that the requested installation was relevant to an ongoing investigation of illegal narcotics activities (R1, 67). It stated that a DEA confidential source indicated that Petitioner obtains multiple kilograms of cocaine from Broward County for distribution on the West Coast of Florida (R1, 68). It also asserted that the

confidential source contacts Petitioner on the listed Metro PCS number (R1, 68).

The standard of showing under 18 U.S.C. Section 2703(d) is lower than that of probable cause. United States v. Madison, 2012 WL 3095357 *10(S.D. Fla. July 30, 2012). Therefore, Petitioner's reliance on case law for the requirements of establishing credibility of a confidential informant's reliability may not be warranted in an application pursuant to section 934.23(5) (IB. 26-27). The affiant in the application did refer to the source as a "DEA confidential source," giving the impression that the confidential source had been working with the DEA. The affiant did not suggest in the application that the source was anonymous. Indeed, Special Agent Marco Moncayo of the Drug Enforcement Administration testified that he received information from an agent in New York that someone in Miami wanted to provide information and that he then met with this person in July of '07 and this person told him about trips that Petitioner had made to Broward to pick up drugs (T3, 87). See J.L. v. State, 727 So. 2d 204, 206 (Fla. 1998)(face-to-face report by informant).

E. Exclusion of Evidence is not a Remedy under Chapter 934

Even if law enforcement did not meet the required standard under section 934.23(5), exclusion of evidence is not a remedy under the statutory scheme. Section 934.28, Florida Statutes

(2007), states that remedies and sanctions described in sections 934.21-934.27 are the only judicial remedies and sanctions for violations of those sections. These sections do not call for suppression of evidence. In Jenkins v. State, 978 So. 2d 116, 130, n. 14 (Fla. 2008), this court stated that it would be inappropriate for the court to read a judicially created remedy of exclusion into a statute that did not call for it. This Court stated that whether evidence obtained in violation of a statute should be suppressed when no constitutional violation occurred turns on the provisions of the specific statute. Jenkins, 978 So. 2d at 128. Notably, federal courts have held that suppression is not a remedy for violation of the Stored Communications Act. See, e.g., United States v. Ferguson, 508 F. Supp. 7, 10 (D.D.C. 2007); United States v. Jones, 2012 WL 6443136 *4 (D.D.C. Dec. 14, 2012); United States v. Hardrick, 2012 WL 4883666 *8 (E.D. La. Oct. 15, 2012).

F. Breadth of Order

Respondent agrees with Petitioner's assertion, based on Joyner v. State, 303 So. 2d 60 (Fla. 1st DCA 1974), that a warrant should not be broader than the affidavit on which it was based, as well as with the statement that law enforcement did not seek CSLI here (IB. 14). In this case, though, acquisition of the CSLI was not by way of a warrant based on an affidavit. It was by way of an order, on which section 934.23(4)(a)(2)

expressly allows an officer to require disclosure of information. An order entered in violation of the terms of section 934.23(5) does not result in suppression of evidence.

G. Inevitable Discovery

The State contends that even if exclusion were a remedy, which it maintains that it is not since Petitioner's Fourth Amendment rights were not violated, Petitioner's location would have been inevitably discovered. The independent source doctrine allows admission of evidence that has been discovered by means wholly independent of any constitutional violation in a case. Nix v. Williams, 467 U.S. 431, 2508-2509, 104 S.Ct. 2501, 81 L.Ed. 2d 377 (1984). In this case, the independent source of "pings" off the co-perpetrator's cell phone independently led law enforcement to Petitioner.

Detective Hendrick pointed out that law enforcement also had a trap and trace on the person Petitioner was meeting, "Vilbon" (T3, 53). He said, "We were able to see that both phones were inside that location [the Miramar address]"(T3, 53). He said that they saw two cars there, one a GMC Envoy with tags that came back to a Cape Coral address (T3, 54). The other vehicle had a temp tag for the East Coast (T3, 54).

Sergeant Cunneen said that he got into his vehicle and headed to Miramar when he saw that Petitioner's phone was in the area of East Broward by US 1 and 595 "[b]ecause Mr. Vilbon's phone

the cell site information that we had on that phone, it remained down in the Hollywood/Miramar area" (T3, 74). At trial, Sergeant Cunneen testified that both phones being watched were in the same general area (T4, 368). He said that there were at least three calls between the two phones once Petitioner started traveling to Broward (T4, 377).

In any event, Petitioner's location would have been inevitably discovered so that exclusion is not warranted. See generally Nix, 467 U.S. at 446-447. Besides the activity on Vilbon's phone, law enforcement was already staked out in Miramar because of previous knowledge of one of Vilbon's houses and his association with Petitioner in providing drugs to take to the West Coast of Florida. Sergeant Cunneen testified that law enforcement had two addresses for Vilbon in Broward County, one in Pompano and one in Miramar (T3, 68). The Miramar address was a few blocks away, less than a mile, from where Vilbon actually was that night (T3, 70). Sergeant Cunneen stated that the traffic out was minimal near the "stash house," between 1:30 and 2:00 in the morning (T3, 71). Law enforcement would have likely detected two cars appearing to travel in tandem in the area, especially with one of them having a Cape Coral tag. See United States v. Orbeoso, 2013 WL 161194 *3-4(D. Ariz. Jan. 15, 2013)(district court applied inevitable discovery doctrine where

defendant's location would have been detected by means other than GPS, including other CSLI information).

H. Good Faith Exception

The order, entered on October 23, 2007, authorizing the installation of a pen register/trap and trace device also directed:

> In accordance with US Title 18, Section 2703(d), it is further Ordered that, Metro PCS their agents and /or the appropriate providers of the wire and/or electronic communications services shall furnish the Broward County Sheriff's Office with historical Cell Site Information indicating the physical locations of the cell sites, along with cell site sectors, utilized for the calls so long as the telephone numbers(s)/facilities, cable or pair and/or electronic serial number remain the same.

(R1, 73).

Section 934.23(4)(a)(2) states that a law enforcement officer may require a provider to disclose a record or other information only when the officer "[o[btains a court order for such disclosure under subsection (5)."

While the information provided by Metro PCS was not information already obtained and maintained at the time of the order, it was information that Metro PCS generated and retained prior to providing it to law enforcement. It is arguably objectively reasonable for the officers to have believed that the lists of "ping" locations given by Metro PCS were historical CSLI within the terms of the order. See generally United States v. Leon, 468 U.S. 897, 922, 104 S.Ct. 3405, 82

L.Ed.2d 677 (1984)(objectively reasonable reliance on a subsequently invalidated warrant cannot justify exclusion).

CONCLUSION

Based on the foregoing discussions, the State respectfully requests this Honorable Court to find that the real time cell site information did not require a statement of probable cause to obtain, that the acquisition of CSLI in this case was not in violation of the Fourth Amendment, that the location of Petitioner's vehicle was inevitable discovery based on the other information available to the officers, and that the officers acted in good faith in light of the order of the magistrate.

CERTIFICATE OF SERVICE

I certify that a copy hereof has been e-filed with the Florida Supreme Court e-filing Portal and furnished by e-mail on March 26th, 2013 to: Tatjana Ostapoff, Assistant Public Defender, at appeals@pd15.state.fl.us; tostapof@pd15.state.fl.us; cgload@pd15.state.fl.us.

CERTIFICATE OF COMPLIANCE

I certify that this brief was computer generated using Courier New 12 point font.

Respectfully submitted and certified,
PAMELA JO BONDI
ATTORNEY GENERAL

/s/ Celia Terenzio
CHIEF ASSISTANT ATTORNEY GENERAL
Fla. Bar No. 656879

/s/ Melynda L. Melear
By: MELYNDA L. MELEAR
ASSISTANT ATTORNEY GENERAL
Fla. Bar No. 765570
Attorney for Respondent, State of Fla.
Office of the Attorney General
1515 North Flagler Drive
Suite 900
West Palm Beach, FL 33401
Primary E-Mail:
CrimAppWPB@myfloridalegal.com
(561) 837-5000
(561) 837-5108(Fax)