#### FILED, 2/24/2013, Thomas D. Hall, Clerk, Supreme Court

## IN THE SUPREME COURT OF APPEAL OF THE STATE OF FLORIDA

SHAWN ALVIN TRACEY,		
Petitioner,		
vs.		CASE NO. SC11-2254
STATE OF FLORIDA,		
Respondent.	/	

# PETITIONER'S INITIAL BRIEF ON THE MERITS

CAREY HAUGHWOUT
Public Defender
15th Judicial Circuit of Florida
Criminal Justice Building
421 Third Street/6th Floor
West Palm Beach, Florida 33401
(561) 355-7600

TATJANA OSTAPOFF Assistant Public Defender

Attorney for Petitioner

# TABLE OF CONTENTS

<u>PAGE</u>
TABLE OF CONTENTS
AUTHORITIES CITED ii
PRELIMINARY STATEMENT
STATEMENT OF THE CASE
STATEMENT OF THE FACTS
SUMMARY OF THE ARGUMENT
ARGUMENT
<u>POINT</u>
THE TRIAL COURT ERRED IN DENYING PETITIONER'S MOTION TO SUPPRESS EVIDENCE DERIVED FROM REAL-TIME CELL PHONE SITE INFORMATION WHICH WAS OBTAINED WITHOUT LEGAL AUTHORITY AND IN VIOLATION OF THE FOURTH AMENDMENT
CONCLUSION
CERTIFICATE OF FONT SIZE
CERTIFICATE OF SERVICE.

# **AUTHORITIES CITED**

<u>CASES CITED</u>	<u>PAGE</u>
Bonilla v. State, 579 So.2d 802 (Fla. 5 <sup>th</sup> DCA 1991)	29
<u>Dozier v. State</u> , 766 So. 2d 1105 (Fla. 2d DCA 2000)	27
(1 la. 2d DCA 2000)	
In re Application by U.S. for an Order Authorizing Installation Register, 415 F.Supp.2d 211 (W.D.N.Y. 2006)	
In re Application of U.S. for an Order Authorizing the Use of a IWL 159187	Pen Register, 2009
(W.D.N.Y. 2009)	17, 19, 20
<u>In re Application of U.S.</u> , 534 F.Supp.2d 585 (W.D. Pa. 2008)	13-14, 17-19
In re Application of U.S. for Orders Authorizing the Installation Registers, 416 F.Supp.2d 390 (D. Mass. 2006)	
In re Application of U.S. for Orders Pursuant to Title 18 U.S F.Supp.2d 76 (D. Mass. 2007)	
<u>In re Application of U. S.</u> , 620 F.3d 304 (11 <sup>th</sup> Cir. 2010)	
<u>John v. State</u> , 534 So.2d 895 (Fla. 5 <sup>th</sup> DCA 1988)	12
<u>Joyner v. State</u> , 303 So. 2d 60 (Fla. 1 <sup>st</sup> DCA 1974)	14

Katz v. United States, 389 U.S. 347	
88 S.Ct. 507, 19 L.Ed.2d 576	
(1967)	21
Mapp v. Ohio, 367 U.S. 643	
81 S.Ct. 1684, 6 L.Ed.2d 1081	
(1961)	28
Mitchell v. State, 25 So.3d 632	
(Fla. 4 <sup>th</sup> DCA 2009)	16, 19
State v. Maynard, 783 So. 2d 226	
(Fla. 2001)	27
State v. Navarro, 464 So. 2d 137	
(Fla. 3d DCA 1984)	12
State v. Setzler, 667 So. 2d 343	
(Fla. 1 <sup>st</sup> DCA 1995)	12
Tracey v. State, 69 So.3d 992	
(Fla. 4 <sup>th</sup> DCA 2011)	17, 20
United States v. Gerber, 994 F.2d 1556	
(11 <sup>th</sup> Cir. 1993)	
United States v. Jones, U.S	
132 S.Ct. 945, 181 L.Ed.2d 911	
(2012)21-25	
United States v. Karo, 468 U.S. 705	
104 S.Ct. 3296, 82 L.Ed.2d 530	
(1984)	
United States v. Knox, 460 U.S. 276	
103 S.Ct. 1081, 75 L.Ed.2d 55	
(1983)	

<u>United States v. Leon</u> , 468 U.S. 897 104 S.Ct. 3405, 82 L.Ed.2d 677 (1984)	28
<u>UNITED STATES CONSTITUTION</u>	
Fourth Amendment	26-27, 28
FLORIDA CONSTITUTION	
Article I Section 23	19
UNITED STATES STATUTES	
18 U.S.C. §2703	16
FLORIDA STATUTES	
Section 934.23(4)	15-16
Section 934.23(5)	16, 26
Section 934.32	15
Section 934.32(2)	15

# OTHER AUTHORITIES CITED

Kevin McLaughlin, The Fourth Amendment and Cell Phone Location Tracking:
Where Are We?
29 Hastings Comm. & Ent. L.J. 421-424
(2007)
W D. If C1, 1 C-: 62.2
Wayne R. Lafave, <u>Search and Seizure</u> §3.3
(3d ed. 1996)

# PRELIMINARY STATEMENT

Petitioner was the defendant in the Criminal Division of the Circuit Court of the Seventeenth Judicial Circuit, in and for Broward County, Florida and the appellant in the Fourth District Court of Appeal. Respondent was the prosecutor and appellee, respectively. In this brief the parties will be referred to as they appear before the Court.

The following symbols will be used:

"R" Record on appeal, followed by the appropriate volume and page numbers

## STATEMENT OF THE CASE

Petitioner was informed against for possession of more than 400 grams of cocaine (Count 1), fleeing and eluding police with lights and siren activated and driving at a high rate of speed (Count 2), driving with a license which had been revoked as a habitual offender (Count 3), and resisting arrest without violence (Count 4) (R1/2-4). His motion to suppress the evidence derived from the use of "real-time" or prospective cell-site information (R1/48-66) was denied, based on the trial court's conclusion that no violation of the Fourth Amendment occurs when the police use cell phone site information to track a defendant's physical location (R1/246-248). The evidence resulting from the tracking of Petitioner's vehicle by the use of real-time cell phone data was admitted at his trial.

Petitioner was tried by a jury (R2/256-257, 259-260), which returned its verdicts finding Petitioner guilty of each count as charged (R2/288, 289, 290, 291). The same day, August 19, 2009, Petitioner was adjudged guilty of Counts 1-4 (R2/292-293) and sentenced to serve the mandatory minimum sentence of fifteen years in prison on Count 1 (R2/295-297), concurrent to a fifteen-year prison term on Count 2 (R2/298-300) and a five-year prison term on Count 3 (R2/301-303). Petitioner was sentenced to time served on Count 4 (R2/292).

On direct appeal, the Fourth District Court of Appeal held that the Fourth Amendment was not offended by the police use of cell phone tracking to follow Petitioner's vehicle. Petitioner's motion for rehearing of the Court's decision was denied on October 14, 2011. He timely filed his notice invoking the jurisdiction of this Court on Monday, November 14, 2011. In its order of January 28, 2013, this Court granted review.

## STATEMENT OF THE FACTS

### MOTION TO SUPPRESS EVIDENCE

On October 23, 2007, Detective Jason Hendrick of the Broward County Sheriff's Office made an application for an order authorizing the installation and use of a pen register and trap and trace device to record inbound and outbound phone calls from and to a specified phone number (R1/67-69). As the factual basis for obtaining the order, the application stated that a confidential source "indicated" that Petitioner "obtains multiple kilograms of cocaine from Broward County" and that the informant "contacts" Petitioner on the cell phone (R1/68).

At the hearing on Petitioner's motion to suppress the evidence, the DEA agent who provided the Sheriff's Office with its information, Marco Moncayo, explained that he was told by another DEA agent in New York that the informant "wanted to provide information to us" (R3/400). Neither the New York agent nor Agent Moncayo had any previous experience with this informant (R1/68, 6/406), who avoided his own arrest and was also paid for his cooperation (R6/407). Moncayo did not know whether the informant was reliable (R6/406). Detective Hendrick further agreed at the hearing that the three-page application for a pen register and trap and trace device did not include any reference to cell phone site information (R1/67-69, 3/41).

The trial judge issued an order granting the application for the pen register and trap and trace device (R1/70-73). The order further directed that the cell phone company provide the Sheriff's Office with "historical Cell Site Information indicating the physical location of cell sites, along with cell site sectors, utilized for the calls so long as the telephone number(s)/facilities; cable and pair and/or electronic serial numbers remain the same" (R1/73). The order did not direct the provision of prospective cell-site information or real-time cell-site information (R1/70-71, 3/43).

After hearing testimony and argument at the hearing on Petitioner's motion to suppress, the trial court further found:

- .... 3. The application for the Order sets forth the legal basis for the installation and use of a pen register/ trap and trace device, but does not contain a sufficient factual basis on which to issue a search warrant.
- 4. On or about December 6, 2007, Investigators received information that the Defendant would be coming to Broward County to purchase cocaine. Investigators used real-time cell-site data obtained by virtue of the Order to track the Defendant as he traveled East across the State and to the general vicinity of the location where he was arrested in the city of Miramar. While there was evidence that the investigators had knowledge of at least one "stash house" used by the Defendant and located within a few blocks of where he was arrested, the State was unable to establish that investigators stationed in the area stumbled upon the Defendant; rather, the evidence demonstrated that it was by

<sup>&</sup>lt;sup>1</sup>The cell phone number changed during the investigation (R6/368).

using the cell phone as a tracking device that they were able to locate him behind the wheel of a GMC Envoy at the intersection of US 441 and Miramar Parkway.

(R2/246-247.)

#### **TRIAL**

During the evening of December 5, 2007, DEA Agent Marco Moncayo monitored and recorded a phone conversation (R6/382, 384) in which Petitioner told someone that "it's small something personal for me" and that he "had someone else's shit" (R6/396-397). In a second phone call that night, Petitioner said again that he had someone else's money tied up and that he had to make a move (R6/398). During its deliberations, this recording was replayed for the jury at its request (R8/639-644).

Police tracked the target phone number purportedly pursuant to the pen register/ trap and trace order obtained in this case (R6/362-363). It was, however, the data relating to the real-time cell-site information which enabled police to pinpoint the location of the phone and thus its user from the west coast of Florida to Broward County (R6/365-366). Using this information, the police determined that they were tracking a red GMC Envoy.

Deputy Eugenio Legra testified that he attempted to make a traffic stop of the GMC Envoy at about 2:00 a.m. on December 6, 2007, by turning on the lights and siren of his marked police car (R5/233)-234). The Envoy did not stop, but pulled

around an Avenger which stopped in front of it. The Envoy accelerated away (R5/236, 372). Legra estimated that the Envoy was moving at about 70 miles, although the speed limit was only 40 miles per hour on SR 7 (R5/242, 270), and he also saw it run a red light at Hollywood Boulevard (R5/238, 271).

Legra followed the vehicle to 59<sup>th</sup> Terrace, where he saw two people bail out of it (R5/242, 244). Legra chased a white male who exited from the front passenger seat (R5/272) and caught him (R5/244-245). The black male who ran from the driver's side of the Envoy was identified as Petitioner (R5/272). When he was taken into custody, he had a cell phone in his hand (R6/416). Two white females were still in the back seat of the Envoy when it was stopped (R5/273). They were later released (R6/440), as was the white male.

The police determined that the Envoy was registered to someone – not Petitioner – who lived in Fort Myers (R6/415). When it was searched, police discovered a kilogram brick of cocaine located inside a purse which was found underneath the spare tire inside the covered spare tire well at the rear of the vehicle (R5/279-280). A glove containing about five ounces of cocaine was also found inside the purse (R5/281, 283). A bag containing \$3000 was recovered from the center console of the Avenger, which had also been stopped by police (R5/295, 353). \$20,000 wrapped in newspaper was found in the Avenger as well (R6/352).

In a conversation tape recorded at the jail (R6/410-411), Petitioner's girlfriend, Tracy Sands, told him that "You slippin so much." Petitioner responded that "You don't know. You don't understand what I was doing" (R6/437). In a second recorded telephone call, Petitioner said that it "ain't like it was in visable [sic] view" and "I didn't know it was there" (R6/456). This recording, too, was replayed for the jury at its request during its deliberations (R8/644-645).

<sup>&</sup>lt;sup>2</sup>This statement was alternatively transcribed as "You know what I mean. But it ain't like it was in visible view, like I know it was there. You know what I mean" (R7/532) and "You know like that area. You know, I mean ain't like it was in visible view, where I know it was in there. You see what I'm saying?"(R8/644-645).

## SUMMARY OF THE ARGUMENT

In the instant case, the State's application for a pen register and/or trap and trace device did not include any request for an authorization to obtain and use real-time cell-site information. The order issued upon the State's application included an authorization for historical cell-site information only. The State's use of real-time cell-site information to find and arrest Petitioner was consequently made without any legal authority. Evidence obtained through the use of the cell-site information should therefore have been suppressed.

Citizens have a reasonable expectation of privacy that their cell phones will not be used as tracking devices. In order to comply with the Fourth Amendment, police seeking to justify any authorization to obtain and use real-time cell-site information are required to establish that there is probable cause to believe that the records would produce evidence of a crime. The State's application in the instant case contained only general and conclusory statements which were insufficient even to establish specific and articulable facts to support the issuance of an order. The exclusionary rule therefore applied to prohibit the introduction of any evidence obtained as a result of the use of real-time cell-site information. The good faith exception to the warrant requirement could not be applied where the State made no attempt to comply with the constitutional requirements.

## <u>ARGUMENT</u>

## <u>POINT</u>

THE TRIAL COURT ERRED IN DENYING Petitioner'S MOTION TO SUPPRESS EVIDENCE DERIVED FROM REAL-TIME CELL PHONE SITE INFORMATION WHICH WAS OBTAINED WITHOUT LEGAL AUTHORITY AND IN VIOLATION OF THE FOURTH AMENDMENT.

### **FACTS**

In the instant case, the Broward County Sheriff's Office submitted an application for an order authorizing the installation and use of a pen register<sup>3</sup> and trap and trace device<sup>4</sup> on a cell phone number used by Petitioner (R67-69). The application sought "to record the inbound and outbound dialed digits from telephone facility (239) 265-2470, helping identify possible co-conspirators." The application was silent about and did not ask to acquire real-time or prospective cell-site information.<sup>5</sup> It was based on information provided to the Sheriff's Office by an

<sup>&</sup>lt;sup>3</sup>A pen register is a device that has the ability to identify *outgoing telephone numbers* dialed on the targeted telephone line. *See* Section 934.02(20), Fla. Stat. (2009).

<sup>&</sup>lt;sup>4</sup>A trap and trace device captures the *incoming telephone numbers* dialed to the targeted telephone line. *See* Section 934.02(21), Fla. Stat. (2009).

<sup>&</sup>lt;sup>5</sup>"Real-time" cell-site information refers to data used by the government to identify, with varying degrees of accuracy, the location of a phone at the present moment. "Real-time" cell-site information is a subset of "prospective cell-site

agent of the federal Department of Drug Enforcement (DEA), who received it from a confidential informant. The DEA agent, Moncayo, had never worked with this informant before (R1/51, 6/406).

The trial court granted the application and issued an order permitting the uses requested by the State (R70-73). In addition, the court's order instructed Metro PCS to provide law enforcement officials with historical cell-site information.<sup>6</sup>

Forty-two days later, the Sheriff's Office monitored real-time or prospective cell-site information being generated by the targeted cell phone. This monitoring

information, which refers to all cell-site information that is generated after the government has received court permission to acquire it. "Historical" cell-site information refers to records stored by the wireless service provider that detail the location of a cell phone in the past (*i.e.*, before the entry of a court order authorizing government acquisition). In re Application of U.S. for Orders Authorizing the Installation and Use of Pen Registers, 416 F.Supp.2d 390, 392 at n. 4 (D. Mass. 2006).

<sup>6</sup>The final paragraph of the court's order states:

In accordance with US Title 18, Section 2703(d), it is further ordered that, Metro PCS their agents and/or the appropriate providers of wire and/or electronic communications services shall furnish the Broward County Sheriff's 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 number(s)/facilities; cable and pair and/or electronic serial number remain the same.

(R1/72-73).

allowed them to trace the physical location of the phone from Fort Myers to Broward County. Ultimately, this tracking led the Sheriff's Office to an address in Miramar, where they saw a GMC Envoy. When they saw Petitioner leave the address in the Envoy, they stopped the vehicle. It was searched, and the cocaine which is the subject of the instant prosecution was recovered.

#### STANDARD OF REVIEW

While a trial court's rulings on factual matters are not generally reviewable, the same is not true for rulings on questions of law. *Cf.*, <u>John v. State</u>, 534 So.2d 895 (Fla. 5<sup>th</sup> DCA 1988). Thus, the *legal effect* of the facts as found by the trial court presents a legal issue, and one on which an appellate court is not required to accord the trial court any overweening deference. <u>State v. Setzler</u>, 667 So. 2d 343, 344-345 (Fla. 1<sup>st</sup> DCA 1995). Where the trial judge misapplies the law to the facts, reversal is required based on the appellate court's *de novo* review of the issue. <u>State v. Navarro</u>, 464 So. 2d 137 (Fla. 3d DCA 1984).

Since the facts pertinent to resolution of the issue in the present case are uncontested, the trial court's legal conclusion that exclusion of the evidence was not required is a question of law which this Court reviews *de novo*.

#### FACIAL OVERBREADTH OF THE AUTHORIZATION ORDER

Apparently completely disregarded by the trial court's denial of Petitioner's motion to suppress was the fact that the pen register/trap and trace application did not seek cell-site information of any kind whatsoever, let alone real-time cell-site information.<sup>7</sup> The order granting the application contains an authorization for the

Cellular telephone networks divide geographic areas into many coverage areas containing towers through which the cell phones transmit and receive calls. Cell phones, whenever on, not automatically communicate with cell towers, constantly relaying their location information to the towers that serve their network and scanning for the one that provides the strongest signal/best reception. This process, called "registration," occurs approximately every seven seconds.

As we change locations, our cell phones automatically switch cell towers. Cellular telephone companies "track the identity of the cell towers serving a phone." When a call is received, a mobile telephone switching office ("MTSO") gets the call and locates the user based on the nearest tower; the call is then sent to the phone via that tower. This process works in reverse when the user places a call. In urban areas, where towers have become increasingly concentrated, tracking the location of just the nearest tower itself can place the phone within approximately 200 feet. This location range can be narrowed by "tracking which 120 degree 'face' of the tower is receiving a cell phone's signal." The individual's location is, however, most precisely determined by triangulating the "TDOA" or "AOA" information of the nearest three cellular towers. Alternatively, the phone can be tracked

<sup>&</sup>lt;sup>7</sup>In its decision in this case, the Fourth District Court of Appeal quoted the explanation of cell-site technology contained in <u>In re the Application of the United States</u>, 534 F.Supp.2d 585, 589-90 (W.D. Pa. 2008) (internal citations and footnotes omitted), *vacated* <u>In re the Application of the United States</u>, 620 F.3d 304 (3d Cir. 2010):

production of *historical* cell-site information, itself never requested by the State.

It is apodictic that a search warrant is invalid to the extent that it authorizes a broader search than the one justified by the affidavit. *E.g.*, <u>Joyner v. State</u>, 303 So. 2d 60, 62 (Fla. 1<sup>st</sup> DCA 1974). The order in the present case is thus overbroad to the extent that it authorizes the production of historical cell-site information. And it is *silent* as to the production of real-time cell-site information, which was accordingly not authorized under the express terms of the order under review. The trial court therefore erred in denying Petitioner's motion to suppress all evidence obtained as a result of the use of real-time cell-site information. There was simply no legal basis for the use of such information by the Broward Sheriff's Office.

THE FOURTH AMENDMENT'S PROTECTION OF THE RIGHT TO A REASONABLE EXPECTATION OF PRIVACY EXTENDS TO THE USE OF REAL-TIME CELL-SITE INFORMATION.

Even had the order granting the State's application in this case provided facially legal authority for the use of the cell-site information, the application which

extremely accurately – within as little as 50 feet – via the built-in global positioning system ("GPS") capabilities of over 90% of cell phones currently in use. [Cellular service providers] store cell tower registration histories and other information . . . [and] now compile and retain extensive personal location information on the subscribers and the cell phones in use.

resulted in its issuance was fatally inadequate to the purpose. Section 934.32, Fla. Stat., provides that a state attorney or assistant state attorney may make an application for a court order authorizing the installation and use of a pen register or trap and trace device, and that the application must include

- (a) The identity of the applicant specified in the section and that identity of the law enforcement agency conducting the investigation, and
- (b) A certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by the investigating agency.

Section 934.32(2).

Not included in this statute is any authorization for the provision of real-time cell-site information, which is obviously not included within the class of incoming or outgoing phone calls which are the object of pen registers or trap and trace devices. Such information is described in Section 934.23(4), Fla. Stat.

- (a) An investigative or law enforcement officer may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber or customer of such service, not including the contents of a communication, only when the investigative or law enforcement officer:
- 1. Obtains a warrant issued by the judge of a court of competent jurisdiction;
  - 2. Obtains a court order for such disclosure

under subsection (5);

- 3. Has the consent of the subscriber or customer for such disclosure; or
- 4. Seeks information under paragraph (b) [relating to phone service records only].

Section 934.23(5), Fla. Stat., provides that a court order for production of such records shall issue only if the law enforcement officer shows "specific and articulable facts showing that there are reasonable grounds to believe that the . . . records of other information sought are relevant and material to an ongoing criminal investigation."

This statute is patterned after the Federal Stored Wire and Electronic Communication and Transactional Records Access Act (SCA), 18 U.S.C. §2703. Thus, both the federal and State statutes provide that they apply to "a record or other information pertaining to a subscriber to or customer of such service, not including the contents of communications." Accordingly, federal law provides guidance for the application of Florida statutes in this area. *See* Mitchell v. State, 25 So.3d 632 (Fla. 4<sup>th</sup> DCA 2009). Moreover, State requirements for electronic surveillance may not provide less protection than federal law.<sup>8</sup> The trial court accordingly held, consistent with In re Application of U.S. for Orders Pursuant to Title 18 U.S.C.

<sup>&</sup>lt;sup>8</sup>The states may provide more protection than the federal law, and indeed Florida law does provide greater protection for the individual with respect to one-party consent to the recording of oral communications.

§2703(d), 509 F.Supp.2d 76 (D. Mass. 2007), that historical cell phone site information is a record or other information pertaining to a subscriber or customer.

As argued by Petitioner below, a clear majority of federal courts have held that the production of real-time cell-site information requires the government to establish the existence of probable cause to believe that the data sought will yield evidence of a crime. *See* cases cited at <u>Tracey v. State</u>, 69 So.3d 992, 999 and notes 8 and 9 (Fla. 4<sup>th</sup> DCA 2011). Thus, <u>In re Application of the United States</u>, 534 F.Supp.2d 585 (W.D. Pa. 2008), the Court held that the definition of electronic communications included in the SCA explicitly *excluded* "Any communication from a tracking device (as defined in s. 3117)" from its scope, and thus did not apply to movement/location information. 534 F.Supp.2d at 601. The conclusion seems inescapable that a cell phone falls within the definition of the term "tracking device" as used in the SCA. <u>In re Application of U.S. for an Order Authorizing the Use of a Pen Register</u>, 2009 WL 159187 at 3 (W.D.N.Y. 2009).

The district court therefore held that such information is governed by the requirement of the Fourth Amendment that police obtain a warrant based upon probable cause before seizing evidence. "This is the standard which the Government has long been required to meet in order to obtain court approval for the installation of a device enabling the Government to record, or 'track,' the movement of a person

or thing." 534 F.Supp.2d at 592. *See*, *e.g.*, <u>United States v. Karo</u>, 468 U.S. 705, 720, 104 S.Ct. 3296, 82 L.Ed.2d 530 (1984).

This ruling is undoubtedly inspired by the recognition that today, we take our cell phones everywhere: to restaurants, theaters and sporting events; to churches, synagogues, and other places of religious worship; to meetings with ex-wives or exhusbands; to business and financial offices; to appointments at psychiatrist's and psychologist's offices; to family planning clinics; to AA and NA meetings; and into our homes and the homes of family members, friends, and personal and professional associates. Many people, especially younger ones, no longer have landline phones, but use cell phones exclusively for all telephonic communication.

The Court's emphasis on the privacy interests that would be invaded by the tracking of cell phone calls is thus not surprising:

Location may reveal, for example, an extra-marital liaison or other information regarding sexual orientation/activity; physical or mental health treatment/conditions (including, e.g., drug or alcohol treatment and/or recovery programs/associations); political and religious affiliations, financial difficulties, domestic difficulties and other family matters (such as marital or family counseling, or the physical or mental health of one's children); and many other matters of a potentially sensitive and extremely personal nature. It is likely to reveal precisely the kind of information that an individual wants and reasonably expects to be private.

534 F.Supp.2d at 587, n. 6. In this aspect, real-time cell-site information is clearly more invasive than historical cell-site information, which can only reveal where the phone user has been; real-time or prospective information, on the other hand, shows where he *is*. 9

Not only does this analysis compel the conclusion that a person has a reasonable expectation of privacy in the location of his cell phone calls, thereby activating his right to the protections of the Fourth Amendment, <u>United States v. Karo</u>, 468 U.S. 705, 104 S.Ct. 3296, it also implicates the constitutional right to privacy guaranteed in Florida by Article I Section 23 of the Florida Constitution. *See also* In re Application of the U.S. for an Order Authorizing Use of a Pen Register, 2009 WL 159187; <u>In re Application by U.S. for an Order Authorizing Installation and Use of a Pen Register</u>, 415 F.Supp.2d 211, 219 (W.D.N.Y. 2006). Certainly, the cases do not authorize the production of real-time cell-site information based solely on the relaxed showing set forth in the pen register/trap and trace statutes of either the

<sup>&</sup>lt;sup>9</sup>The fact that real-time cell-site information reveals a target's present location distinguishes the instant case from the historical cell-site information which was at issue in Mitchell v. State, 25 So.3d 632 (Fla. 4<sup>th</sup> DCA 2003), in which the Fourth District Court of Appeal held that retrieval of such information did not implicate the Fourth Amendment, based on In re Application of U.S. for Orders Pursuant to Title 18 U.S.C. §2703(d), 509 F.Supp.2d 76 (D. Mass. 2007).

state or federal government.<sup>10</sup> Indeed, in <u>In re Application of U.S. for an Order Authorizing Use of a Pen Register</u>, 2009 WL 159187 at 1, the Government conceded that the pen register statute alone could not authorize the order sought.

Petitioner recognizes that the Third Circuit Court of Appeals has vacated the decision in In re the Application of the United States, 534 F.Supp.2d 585. In In re the Application of the United States, 620 F.3d 304 (3d Cir. 2010), the circuit court of appeal emphasized that the Government in that case sought production of historical (not real-time) cell-site information. 620 F.3d at 311. It further relied, as did the Fourth District Court of Appeal below, Tracey, 69 So.3d at 995, on the prior decision of the United States Supreme Court in United States v. Knox, 460 U.S. 276, 103 S.Ct. 1081, 75 L.Ed.2d 55 (1983) which held that citizens have no reasonable expectation of privacy in the movement of their vehicles on public highways. Compare United States v. Karo, 468 U.S. 705, 104 S.Ct. 3296, 82 L.Ed.2d 530 (1984), holding that the placement of a tracking device in a chemical drum in order to ascertain the drum's presence inside a residence required a warrant supported by probable cause: monitoring the beeper "indicated that the beeper was inside the house, a fact that could not have been visually verified." Id. at 715, 104 S.Ct. 3296.

<sup>&</sup>lt;sup>10</sup>See Kevin McLaughlin, The Fourth Amendment and Cell Phone Location Tracking: Where Are We? 29 Hastings Comm. & Ent. L.J. 421-424 (2007).

This analysis has, however, been called into question by the recent decision of the United States Supreme Court in <u>United States v. Jones</u>, \_\_ U.S. \_\_\_\_, 132 S.Ct. 945, 181 l.Ed.2d 911 (2012). There, the Court addressed whether the Government's installation of a GPS tracking device on a vehicle constituted a search within the meaning of the Fourth Amendment. Five Justices joined Justice Scalia in finding that the placement of the device on the vehicle amounted to a trespass and thus a search within the original meaning of the Fourth Amendment.

Justice Scalia specifically emphasized, however, that this analysis was the most restrictive which was necessary to resolve the issue in the case and did not limit the "reasonable expectation of privacy" analysis which was announced in <u>Katz v. United</u> <u>States</u>, 389 U.S. 347, 360, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967) ("the Fourth Amendment protects people, not places," 389 U.S. at 351, 88 S.Ct. 507). Thus, Justice Scalia cautioned that

unlike the concurrence, which would make *Katz* the exclusive test, we do not make trespass the exclusive test. Situations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* analysis.

(Emphasis original.)

In counterpoint to the trespass analysis of Justice Scalia, four Justices joined in Justice Alito's concurring opinion which finds that the Fourth Amendment is implicated whenever a person's reasonable expectation of privacy is violated, regardless of the existence of any property interest in the invaded place. 132 S.Ct. at 960. Justice Alito and the three Justices who joined him observed under this analysis that

Recent years have seen the emergence of many new devices that permit the monitoring of a person's movements...

Perhaps most significant, cell phones and other wireless devices now permit wireless carriers to track and record the location of users — and as of June 2011, it has been reported, there were more than 322 million wireless devices in use in the United States. [Footnote omitted.] . . . . The availability and use of these and other new devices will continue to shape the average person's expectations about the privacy of his or her daily movements.

132 S.Ct. at 963. In contrast to the "pre-computer age," when long-term surveillance was "difficult and costly and therefore rarely undertaken," "devices like the one used in the present case, however, make long-term monitoring relatively easy and cheap." *Id.* at 963-64. Absent legislative action, "The best that we can do in this case is to apply existing Fourth Amendment doctrine and to ask whether the use of GPS tracking in a particular case involved a degree of intrusion that a reasonable person

would not have anticipated." *Id.* at 964. Using this framework, Justice Alito had no difficulty in concluding that the four-week long monitoring in <u>Jones</u> constituted a search under the Fourth Amendment. *Id.* 

Critically, Justice Sotomayor concurred in the majority opinion because she agreed that

When the Government physically invades personal property to gather information, a search occurs. The reaffirmation of that principle suffices to decide this case.

132 S.Ct. at 955. Resolution of the case because of the Government's physical trespass to the vehicle thus "supplies a narrower basis for decision." *Id.* at 957.

Nevertheless, Justice Sotomayor agreed with Justice Alito that times had changed:

With increasing regularity, the Government will be capable of duplicating the monitoring undertaken in this case by enlisting factory- or owner-installed vehicle tracking devices or GPS-enabled smart phones [citation omitted]. . . . As Justice ALITO incisively observes, the same technological advances that made possible nontrespassory surveillance techniques will also affect the *Katz* test by shaping the evolution of societal privacy expectations. . . . Under that rubric, I agree with Justice ALITO that, *at the very least*, "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."

Id. at 955 (emphasis added). Justice Sotomayor went on to caution against the

dangers inherent in even short-term monitoring, where

some unique attributes of GPS surveillance relevant to the Katz analysis will require particular attention. monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. See e.g., People v. Weaver, 12 N.Y.3d 433, 441-442, 882 N.Y.S.2d 357, 909 N.E.2d 1195, 1199 (2009) ("Disclosed in [GPS] data . . . will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDs treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on"). The Government can store such records and efficiently mine them for information years into the future. [Citation omitted.] And because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: "limited police resources and community hostility."

132 S.Ct. at 955-56. Finally, Justice Sotomayor wisely warns against the chilling of associational and expressive freedoms which may result because of awareness that the Government may be watching. *Id.* at 956.

The net result is that GPS monitoring – by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track – may "alter the relationship between citizen and government in a way that is inimical to democratic society." [Citation omitted.]

*Id.* at 956.

Based on these considerations, Justice Sotomayor stated her willingness to reconsider whether a reasonable societal expectation of privacy in the public movements of citizens existed regardless of whether the Government could obtain the same information through lawful conventional surveillance means or whether the information is voluntarily disclosed to third parties. *Id.* at 956-57.

It is evident, than, that a majority of the Justices agree that the kind of surveillance which occurred in the present case raises grave concerns for the privacy rights of citizens and is consequently governed by Fourth Amendment analysis. This conclusion is in line with that reached by the clear majority of federal courts. The ruling of the district court of appeal below to the contrary is based on a too-restrictive reading of the federal authorities and must be rejected.

THE APPLICATION IN THE INSTANT CASE WAS INADEQUATE UNDER ANY STANDARD.

In the present case, the application submitted to the trial court entirely failed to state probable cause for the issuance of an order authorizing the use of cell-site information. The application states:

A DEA Confidential Source (CS) indicated that Shawn Alvin Tracey obtains multiple kilograms of cocaine from Broward County for distribution on the West Coast of Florida. Furthermore, the CS contacts Shawn Tracey on the listed Metro PCS number.

(R1/68).

These two generalized and conclusory sentences do not establish even the "specific and articulable facts" which constitute the *minimum* showing which must be made to support an authorization to use cell-site information. The statement does not explain the origin of the informant's information; whether it was based on first-hand knowledge or was merely hearsay obtained from some other source; when Petitioner was supposed to have last engaged in the alleged criminal conduct; when he was supposed to again engage in the alleged criminal conduct; or how the cell phone was involved in the transactions.

Critically, the statement did not demonstrate in any way that the confidential source was reliable. This was not surprising, since the Broward deputies, like the DEA agent himself, had no way of knowing whether the informant was reliable: he was a first-time source, unknown to any of them, and had no history of providing reliable information to any law enforcement agency (R5/406).

Information provided by a criminal or anonymous source is insufficient, absent a demonstration of his reliability, to constitute "articulable facts" supporting a Fourth

<sup>&</sup>lt;sup>11</sup>Section 934.23(5), Fla. Stat.

## Amendment intrusion:

[T]he courts have quite properly drawn a distinction between [informers likely to have been involved in the criminal activity] and the average citizen who by happenstance finds himself in the position of a victim of or a witness to criminal conduct and thereafter relates to the police what he knows as a matter of civic duty. One who qualifies as the latter type of individual, sometimes referred to as a "citizen-informer," is more deserving of a presumption of reliability than the informant from the criminal milieu.

State v. Maynard, 783 So. 2d 226, 230 (Fla. 2001) *quoting* Wayne R. Lafave, Search and Seizure §3.3 (3d ed. 1996). Where the State presents no evidence to show its informant's veracity, reliability, or basis of knowledge, it fails to demonstrate by specific and articulable facts that its actions were legally permissible. Dozier v. State, 766 So. 2d 1105, 1105 (Fla. 2d DCA 2000) ("In addition to the lack of information regarding the informant's veracity and reliability, it is significant that the record fails to show how the informant knew what she claimed to know").

In the instant case, the application for the use order likewise did not state any grounds for believing that the unnamed informant was reliable, did not suggest that he was in any way a "citizen-informant," and did not even show how the informant knew what he/she claimed to know.<sup>12</sup> The application therefore completely failed to

<sup>&</sup>lt;sup>12</sup>In fact, the informant used in this case was a paid informant who also avoided arrest for his own criminal activity (R5/407).

state even specific and articulable facts, let alone probable cause, which is required to justify the issuance of an order permitting the use of real-time cell-site information.

THE EXCLUSIONARY RULE REQUIRES SUPPRESSION OF THE EVIDENCE OBTAINED AS A RESULT OF THE UNAUTHORIZED USE OF REAL-TIME CELL-SITE INFORMATION IN THIS CASE.

Once it has been established that the order authorizing the use of the cell phone information in this case was improperly issued, the exclusionary rule ordinarily operates to prevent the admission into evidence of information which is obtained by the police in violation of the Fourth Amendment. Mapp v. Ohio, 367 U.S. 643, 81 S.Ct. 1684, 6 L.Ed.2d 1081 (1961). A good faith exception to the exclusionary rule exists to permit the introduction of evidence obtained during the execution of a search warrant which is later determined to be deficient if the officers' reliance on the warrant was objectively reasonable and in good faith. United States v. Leon, 468 U.S. 897, 921-925, 104 S.Ct. 3405, 82 L.Ed.2d 677 (1984). See also United States v. Gerber, 994 F.2d 1556 (11th Cir. 1993). Since the original order obtained by the State in this case was not based upon any assertion of either probable cause or even reasonable grounds, no good faith on the part of the police, who entirely failed to comply with the statutory and constitutional requirements, can be asserted. E.g.,

Bonilla v. State, 579 So.2d 802 (Fla. 5th DCA 1991).

Consequently, in view of the State's total failure to establish probable cause or provide specific and articulable facts to believe that production of the real-time cell tower site information sought by the police in the instant case would produce evidence of a crime, or indeed to even obtain an order which authorized the use of such information, the evidence obtained as a result of the real-time cell-site information should have been suppressed.

# **CONCLUSION**

Based upon the foregoing argument and the authorities cited therein, Petitioner requests that this Court reverse the judgment and sentence below and remand this cause with directions to grant Petitioner's motion to suppress the evidence.

Respectfully submitted,

CAREY HAUGHWOUT
Public Defender
15th Judicial Circuit of Florida
Criminal Justice Building
421 Third Street/6th Floor
West Palm Beach, Florida 33401
(561) 355-7600
appeals@pd15.state.fl.us

/s/ Tatjana Ostapoff
TATJANA OSTAPOFF
Assistant Public Defender
Florida Bar No. 224634

Attorney for Petitioner

# **CERTIFICATE OF FONT SIZE**

I HEREBY CERTIFY that this brief has been prepared in 14 point Times New Roman font, in compliance with Fla. R. App. P. 9.210(a)(2).

/s/ Tatjana Ostapoff
Assistant Public Defender

# **CERTIFICATE OF SERVICE**

I HEREBY CERTIFY that a copy hereof has been furnished to Sue-Ellen Kenney, Assistant Attorney General, 1515 N. Flagler Drive, ninth floor, West Palm Beach, Florida 33401 by e-mail at <a href="mailto:CrimAppWPD@myfloridalegal.com">CrimAppWPD@myfloridalegal.com</a> this 22d day of FEBRUARY, 2013.

/s/ Tatjana Ostapoff
Of Counsel