UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

Case No. 12-cr-20052

v.

HONORABLE STEPHEN J. MURPHY, III

CARLOS POWELL, et al.,

Defendants.
_____/

ORDER DENYING MOTION TO SUPPRESS BY DEFENDANTS CARLOS POWELL (D-1)**, ERIC POWELL** (D-2)**, EARNEST PROGE** (D-5)**, TOBIAS PROGE** (D-6)**, TAMIKA TURNER** (D-8)**, MARGARITA DE VALLEJO** (D-10)**, BENNY WHIGHAM** (D-11)**, AND DONALD WILSON** (D-12) (docket no. 74)

TABLE OF CONTENTS

INTRODUCTION

This is a criminal drug prosecution. Defendants are charged with various drug dealing, firearms, and money laundering offenses. 21 U.S.C. §§ 841(a)(1) and 846; 18 U.S.C. §§ 924(c)(1) and 1956. The government contends that the defendants operated a large scale drug trafficking ring in Detroit and, among other things, imported large quantities of cocaine and heroin into the city.

In April 2012, eight of the fourteen defendants filed a Motion to Suppress Evidence and Request for an Evidentiary Hearing. *See* Mot. to Supress, ECF No. 74; *see also* Notices of Joinder/Concurrence, ECF Nos. 81, 87, 88, 94. The Court held a hearing on the motion on December 18, 2012. On January 4, 2013, the Court issued an order (1) making a preliminary finding that defendants Carlos Powell and Eric Powell had standing to contest admission of the evidence challenged in the motion; (2) denying the motion as to the challenged pen-register and trap-and-trace evidence; and (3) ordering an evidentiary hearing regarding federal agents' use of a GPS tracking device without a warrant during the investigation. *See* Order Denying in Part Mot. to Suppress ("Order"), ECF No. 167. The Court conducted the evidentiary hearing on January 17, 2013 and February 12, 2013. For the reasons stated at the hearing and explained below, the Court will deny the remainder of the motion to suppress in full.

LEGAL STANDARD

The Fourth Amendment provides that "[t]he right of the people to be secure . . . against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const.

amend. IV. The Amendment protects "people — and not simply 'areas' — against unreasonable searches and seizures." *Katz v. United States*, 389 U.S. 347, 353 (1967). A valid search or seizure "requires adherence to judicial processes," and searches without a warrant are "per se unreasonable under the Fourth Amendment." *Id*. at 357.

To help protect an individual's Fourth Amendment rights, courts apply the "exclusionary rule," which provides that evidence obtained in violation of the Fourth Amendment will be excluded from use against a defendant at trial. *United States v. Clariot*, 655 F.3d 550, 553 (6th Cir. 2011). A judicial rule, it is premised on "deterrence — to discourage the police from violating the Fourth Amendment by prohibiting them from leveraging illegal encounters into criminal convictions." *Id*.; *see also Elkins v. United States*, 364 U.S. 206, 217 (1960). Because the rule is judicial in source, not constitutional, and is intended to deter government misconduct, evidence is not always excluded when the Fourth Amendment has been violated. For example, an exception to the rule occurs when an officer conducts an unconstitutional search in "good faith reliance on some higher authority, such as a warrant or a statute, even if the warrant or statute were later held invalid or unconstitutional." *United States v. Buford*, 632 F.3d 264, 271 (6th Cir. 2011), *cert. denied*, 132 S. Ct. 370 (2011). In that event, the evidence, though seized unconstitutionally, nonetheless remains admissible because there is no bad-faith conduct by the officer to deter. *Id.*

BACKGROUND

On April 15, 2012, defendants Carlos Powell (D-1), Eric Powell (D-2), Earnest Proge (D-5), and Benny Whigham (D-11) filed a Motion to Suppress and Request for an Evidentiary Hearing. Following the motion, co-defendants Margarita de Vallejo (D-10),

Tobias Proge (D-6), Tamika Turner (D-8), and Donald Wilson (D-12) filed notices of joinder and concurrence. *See* Notices of Joinder/Concurrence.[1] The remaining defendants did not join the motion. Since the motion's filing, Juan Valle (D-9) entered a guilty plea on January 31, 2013. Valle was not a party to the suppression motion, but Defendants indirectly challenge the search of his vehicle in the motion.

Defendants challenge the admission of the following the evidence:

(1) Pen-register and trap-and-trace data acquired via orders issued over a nine-month period, for cellular telephones used by Carlos Powell, Eric Powell, and Juan Valle. The Court denied Defendants' motion to suppress this evidence on January 4, 2013. Order at 13.

(2) Real-time cell-site location data acquired via Criminal Rule 41 search warrants issued between March 11, 2010 and October 5, 2010, for six cellular telephones. *See* Fed. R. Crim. P. 41.

(3) Location data acquired over a period of several months through the warrantless use of a GPS tracking device affixed to vehicles owned and operated by Carlos Powell and Eric Powell.

(4) Evidence seized during the warrantless search of vehicles belonging to Benny Whigham, Juan Valle, Earnest Proge, and Margarita de Vallejo, incident to traffic stops.

(5) Evidence seized during the search of nine properties in the Detroit metro area, pursuant to search warrants.

[1] For the purposes of this order, the Court will refer to the eight moving defendants as "Defendants."

DISCUSSION

I. Standing

Fourth Amendment rights "may not be vicariously asserted." *United States v. Pearce*, 531 F.3d 374, 381 (6th Cir. 2008) (quoting *Rakas v. Illinois*, 439 U.S. 128, 133-34 (1978)). To assert a Fourth Amendment violation, a person must first "demonstrate a reasonable expectation of privacy in the things seized." *United States v. Smith*, 263 F.3d 571, 582 (6th Cir. 2001). Criminal "[c]o-conspirators and codefendants have been accorded no special standing." *United States v. Williams*, 354 F.3d 497, 511 (6th Cir. 2003) (quoting *United States v. Padilla*, 508 U.S. 77, 81–82 (1993)).

Because of the "omnibus" nature of the motion to suppress, which was filed collectively by eight defendants and challenges dozens of searches and seizures of many different (moving and non-moving) defendants' properties, the Court initially questioned whether each moving defendant had standing to challenge the searches at issue. The government argued that, because the cell phones, vehicles, and properties in dispute were not the co-property of all Defendants, only a few of the defendants — those with direct privacy interests in the things searched — have the ability to challenge the evidence at issue.

In its January 4, 2013 Order, the Court analyzed the standing question at some length. The Court concluded that Defendants do not challenge each search directly as unconstitutional. Rather, Defendants directly challenge the cell phone location and vehicle-tracking searches as unconstitutional, and then argue that evidence seized in every subsequent search was the "fruit" of those initial unconstitutional searches, and therefore inadmissible. Because Carlos and Eric Powell owned the cell phones and vehicles at issue,

the Court concluded that they have standing to challenge all the searches at issue in the motion, either directly or derivatively. Order at 7 (citing *Wong Sun v. U.S.*, 371 U.S. 471 (1963)). The remaining Defendants lack standing, and therefore all of the challenged evidence is admissible against them at trial, regardless of the Court's decision on this motion.

At the January 17, 2013 hearing, the government raised an additional argument that, with respect to the GPS tracking device affixed to Eric Powell's truck, Powell was the truck's sole owner and operator, and therefore the only defendant with standing to challenge the search. *See* Hr'g Tr., Jan. 17, 2013 at 6 ("Hr'g I"), ECF No. 176. The Court offered the opportunity for additional written argument on the issue, and, after examining two letters from counsel and various exhibits, the Court, for the reasons stated on the record at the February 12, 2013 hearing, found that Carlos Powell also has standing to challenge the search of the truck, and resolved the procedural questions relevant to the issue. *See* Hr'g Tr., Feb. 12, 2013 ("Hr'g II"), (No ECF Citation yet available).

The Court will now address the motion to suppress with respect to each remaining category of evidence: (1) the cell-site location data; (2) the location data derived from the use of a GPS tracking device; (3) evidence seized during traffic stops of Whigham, Valle, Proge, and de Vallejo's vehicles; and (4) evidence seized during the search of nine properties in the Detroit area.

II. Real-Time Cell-Site Location-Data Warrants

Defendants challenge search warrants authorizing collection of real-time cell-site location data from six cellular telephones owned by Carlos Powell, Eric Powell, and Juan Valle. The collection of real-time cell-site location data gives the government the ability to

learn and follow the actual physical location of each phone at any time. Warrants authorizing the searches were issued on March 11, 2010; March 31, 2010; May 7, 2010; June 17, 2010; and October 5, 2010. Each warrant authorized the Drug Enforcement Administration ("DEA") to obtain real-time location data for up to thirty or forty-five days after the warrant issued. Defendants argue that the warrants issued without probable cause.

A. Technical Background

Every cellular telephone is capable of being located in one of two ways: by cell-site tracking, or by GPS signal locating. The first, cell-site tracking, exploits a cell phone's need to connect to a cellular network. To function, a cell phone must be in contact with a cell tower to transmit calls, text messages, and the like. A cell phone, once activated, will automatically search for the closest cell tower. Once the phone locates a tower, it submits a unique identifier — its "registration" information — to the tower so that any outgoing and incoming calls can be routed through the correct tower. This search and submission of information occurs every several seconds. If a signal to or from a tower changes strength, or the cell phone moves, the cell phone may switch its registry to a different tower. *See* Timothy Stapleton, Note, *The Electronic Communications Privacy Act and Cell Location Data*, 73 Brook. L. Rev. 383, 387 (2007). This fact, combined with the fact that in a typical urban environment, a cell phone will be in range of and submit information to several cell towers simultaneously, makes it possible to calculate a cell phone's location within anywhere from several blocks to a few feet using the mathematical process of

"multilateration."[2] While the precision of location data may vary, recent FCC regulations to enable law enforcement to identify a phone's location during a 911 call require a range of precision of no greater than 125 meters. *See* Wayne LaFave, *Search and Seizure*, § 2.7(f) (5th ed.). Law enforcement can artificially speed up the process by "pinging" a cell phone, that is, sending an electronic signal to a target cell phone — such as by dialing a number and hanging up — that triggers an identification transmission from the phone. Thus, law enforcement can obtain location data from a cell phone at will. *See, e.g.*, *United States v. Forest*, 355 F.3d 942, 947 (6th Cir. 2004), *cert. granted, judgment vacated sub nom. Garner v. United States*, 543 U.S. 1100 (2005).

More recently, most "smart" phones now come equipped with GPS locators, often for mapping applications, that can identify a phone's location by using a built-in GPS device. By obtaining the GPS device's information, an even more precise record of the cell phone's location may be obtained without resorting to "multilateration" calculations. *See* Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 Md. L. Rev. 681, 713 (2011). In both the "cell-site location" or "GPS location" situations, the government can either track a person in real-time using live registration or GPS data, known as "prospective" records; or compile a list of a person's recent movements with their cell phone, known as "historic" records. *See* Stapleton*, supra,* at 388. In either case, if a cell phone is not turned on, it cannot transmit any data.

[2] The concept is often referred to as "triangulation," but because the process may involve more or fewer than three cell towers, "multilateration" is a more accurate term. *Id.*

For the purposes of the remainder of this opinion and order, the Court will refer to cell-phone location data gathered in real time, whether compiled by multilateration or GPS tracking, as "real-time cell-site location data."

B. Legal Standards

Defendants challenge all of the search warrants for cell-site and GPS location data, but their primary challenge is to the March 11, 2010 warrant authorizing collection of real-time cell-site location data for the phone number (313) 529-5848, subscribed to by Carlos Powell. Defendants argue that the warrant was not supported by probable cause, and the subsequent warrants are the "fruit of the poisonous tree" of that original warrant.[3] Their probable-cause and fruit-of-the-poisonous-tree arguments with respect to the March 11, 2010 warrant are generally applicable to all the real-time cell-site location data warrants at issue in this case. The government argues that the affidavits submitted to the magistrate judge contained enough facts to establish a probable-cause basis for the warrants to issue; and that even if they did not, the evidence should not be suppressed because the DEA agents relied in good faith on the warrants.

Before discussing the March 11, 2010 warrant application, the Court will consider the antecedent question of what legal standard applies to a government application to obtain real-time cell-site location data, and what showing, if any, the government must make to acquire the data. As set forth below, the Court concludes that the government must establish probable cause for long-term, real-time tracking of an individual via his cell phone, and that a specific showing must be made to establish probable cause for such tracking.

[3] Defendants' initially challenged the March 31, 2010 warrant, but then shifted to the March 11, 2010 warrant when it became clear it was the first cell-phone warrant issued.

1. History of Real-Time Cell-Site Location Data Authorization

The act of tracking an individual's movements in real time is neither new, nor dependent on modern technology. The tried-and-true method of simply following a suspect on foot stretches back many years; real-time tracking of John Dillinger's associates in the 1930s occurred when FBI agents sat in cars and restaurants following their quarry. Thirty years ago, long before cell phones became common, the Supreme Court held in *United States v. Knotts*, 460 U.S. 276 (1983), that a radio beeper tracking device could be used to track a criminal suspect in public. Today, however, real-time tracking involves far more technologically sophisticated and geographically precise tracking methods; as well as the development that in many cases, a tracked individual owns the very device being used to track him.

2. Statutory Authorities

The government may lawfully acquire many different types of data from electronic devices like cell phones, from as little as a phone's subscriber information to as much as the contents of conversations between two people. Currently, federal statutes authorize four means of collecting such data: pen-register and trap-and-trace devices, access to stored communications, the use of tracking devices, and real-time communication intercepts (a.k.a. "wiretaps"). Wiretapping authority was first authorized as part of the Omnibus Crime Control and Safe Streets Act of 1968, P.L. 90-351, 82 Stat. 197; the remaining authorizations are part of the Electronic Communications Privacy Act ("ECPA") of 1986, P.L. 99-508, 100 Stat. 1848.[4]

[4] These statutes have been amended from time to time; for example, by the Communications Assistance and Law Enforcement Act of 1994, P.L. 103-414, 108 Stat. 4279, and the USA PATRIOT Act, P.L. 107-56, 115 Stat. 272.

a. Pen Registers and Trap-and-Trace

Pen-register and trap-and-trace orders are the most easily obtainable. As discussed in the Court's January 4 Order, a pen-register / trap-and-trace ("pen / trap") order captures the incoming and outgoing numbers dialed by a phone (or other such non-communication-content data transmitted by electronic devices). To obtain this information, the government need only certify that "the information likely to be obtained by [] installation [of a pen register or trap and trace device] and [its] use is relevant to an ongoing criminal investigation." *See* 18 U.S.C. §§ 3122(b)(2) and 3123(a)(1); *see also Michigan Bell Tel. Co. v. United States*, 565 F.2d 385, 388 (6th Cir. 1977).

b. Stored Communications Act

Acquisition of stored electronic communications (including stored internet communications and cell-phone subscriber records) is governed by the Stored Communications Act ("SCA"). *See* 18 U.S.C. §§ 2701-2712. The SCA generally prohibits providers of electronic communication services or remote computing services from disclosing information to the government, and provides three ways for the government to obtain records. For records and communications created less than 180 days before the date of application, the government must obtain a search warrant to retrieve the information. *See* 18 U.S.C. § 2703(a). For older records and communications, the government must obtain a court order based on "specific and articulable facts" that provide "reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." *See* 18 U.S.C. § 2703(d); *Warshak v. United States*, 532 F.3d 521, 534 (6th

Cir. 2008). The government may also obtain stored records via a properly issued and served subpoena from federal grand jury or district court.

c. Tracking Devices under 18 U.S.C. § 3117

A "tracking device" is an "electronic or mechanical device which permits the tracking of the movement of a person or object." 18 U.S.C. § 3117(b). The beepers discussed in *Knotts* are one example. *See Knotts*, 460 U.S. at 278. The government may install and use tracking devices under the authority of 18 U.S.C. § 3117. A search warrant issued upon a showing of probable cause is required. Criminal Rule 41 contains specific provisions to authorize installation of a tracking device. 18 U.S.C. § 3117(a); Fed. R. Crim. P. 41(b)(4); *see Forest*, 355 F.3d at 949.

d. Wiretaps

Finally, the authority to use wiretaps — government interception of real-time communications, such as the voices on a call or the text in an instant message — is codified at 18 U.S.C. §§ 2510-2522, also known as "Title III" for its place in the 1968 Act. *See United States v. Alfano*, 838 F.2d 158, 161 (6th Cir. 1988). To wiretap individuals, the government makes a showing of what is sometimes referred to as "probable cause plus." In addition to the conventional probable-cause showing, the "plus" showing requires that an applicant declare whether or not "investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous." *See* 18 U.S.C. § 2518(3)(c). The wiretap statute reaches only "electronic communications," and it explicitly excludes "tracking devices" under 18 U.S.C. § 3117. *See* 18 U.S.C. § 2510(12)(C).

3. Judicial Precedent

Federal courts considering issues involving real-time cell-site location data usually follow one of two approaches. The majority of jurisdictions require the government to make a probable-cause showing to obtain real-time cell-site location data. While some courts also require the same showing for historic cell-site location data, most other courts find that historical location data are "stored communications" and may be obtained on a lesser "relevant to an ongoing criminal investigation" showing. The minority of jurisdictions do not accord any protection to cell-site information, or they authorize the use of such information on a showing of less than probable cause. And, finally, some jurisdictions have not addressed the issue.

a. Cases in Which Probable Cause Is Required

Of the courts that have addressed the issue, a significant majority have required the government to make a showing of probable cause before obtaining real-time cell-site information. One of the first major decisions to address the issue of cell-site location information was *In re Authorizing the Use of a Pen Register*, 384 F. Supp. 2d 562 (E.D.N.Y. 2005). When considering an application for an order authorizing collection of cell-site location data, the court found that while cell-site location information is similar to information that a pen register would provide, the government could not obtain the information merely on the showing required by the pen register statute. *Id.* at 564. After engaging in statutory construction, including a review of legislative history, the court determined that nothing less than probable cause would permit the release of this information. *See id.* at 565 (citing testimony before the U.S. House of Representatives that "the authority for pen registers and trap and race devices cannot be used to obtain tracking or location information other than that which can be determined from the phone number").

The court granted the government's motion for reconsideration of its original decision. *See In re Application of the U.S. for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device*, 396 F. Supp. 2d 294 (E.D.N.Y. 2005). The court also invited Electronic Frontier Foundations ("EFF") to submit a brief as an amicus curiae. The government again argued that cell-site information could be obtained on a showing of less than probable cause; EFF argued that such information requires a showing comparable to the wiretap "super-warrant" requirement. *Id.* at 305. The court again concluded that the probable-cause standard governed the request for the information. *See id.* at 322.

Notably, the court did not specifically hold that Fourth Amendment protections apply to cell-site information, *see id.* at 323, or that the probable-cause standard would necessarily suffice in the future, and the court declined to address whether a "super-warrant" requirement for the information was appropriate. *See id.* at 322. The procedural posture of the case obviated any requirement for the court to directly decide the extent of the privacy interests at stake; the court merely considered an *application* to obtain data, and therefore considered the issues *before* any information was gathered.[5]

Another frequently cited case, *In re Application for Pen Register and Trap/Trace Device with Cell-site Location Authority*, 396 F. Supp. 2d 747 (S.D. Tex. 2005), considered existing privacy statutes and concluded that use of real-time cell-site location data should be considered equivalent to the use of a "tracking device" governed by 28 U.S.C. § 3117 and employed a probable-cause standard. *See id.* at 757. Looking to the ECPA, the court concluded that the provisions of the ECPA do not overlap; and therefore, cell-site

[5] Here, in contrast, Defendants filed a motion to suppress *after* the government collected the data, which demands a more extensive review of the interests in the case.

information should be governed by the probable-cause standard *only* and not other ECPA provisions with alternate standards. *Id.* at 757-59.

Five years later, the same court extended Fourth Amendment protection to historic cell-site information. *In re Application of the United States for Historical Cell-site Data*, 747 F. Supp. 2d 827 (S.D. Tex. 2010). The court compared historical cell-site data to the GPS device used in *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010), *aff'd in part sub nom. United States v. Jones*, 132 S. Ct. 945 (2012), and concluded that although *Maynard* dealt with a slightly different tracking technology, the historical cell-site data at issue in the case was actually *more* intrusive than the GPS data revealed in *Maynard*. *See id.* at 840-41. The court pointed out that while the level of detail provided by cell-site technology is close to that of GPS technology, cell-site technology is more reliable than GPS technology, and because cell phones are generally carried on the person, it captures more revealing information than GPS technology. *Id.*

Several other jurisdictions agree that cell-site information may not be obtained by the government absent some showing of probable cause. *See, e.g.*, *In re Application of the United States for an Order Authorizing the Disclosure of Prospective Cell-site Information*, No. 06-MISC-004, 2006 WL 2871743, at *5 (E.D. Wis. Oct. 6, 2006) (finding it "clear" that the effect of cell-site information is akin to a "tracking device," and noting that Criminal Rule 41 is the standard procedure for the use of mobile tracking devices); *see also id.* at *4 n.3 (noting that the government "regularly" requests cell-site information under the "super-warrant" requirements of § 2518), *cf. id.* at *5 n.6 (suggesting it was "doubtful" that the use of cell-site data for tracking would be considered a Fourth Amendment search); *In re Application of the United States for an Order Authorizing the Monitoring of Geolocation*

and Cell-site Data . . ., No. 06–0186, 187, 188, 2006 WL 6217584, at *4 (D.D.C. Aug. 25, 2006) (agreeing with the "majority rule" that Criminal Rule 41 governs the request for prospective cell-site information and finding a Fourth Amendment privacy interest in location); *In re Application of United States for an Order Authorizing Disclosure of Location Information*, 849 F. Supp. 2d 526, 539-42 (D. Md. 2011) (finding that "the subject here has a reasonable expectation of privacy both in his location as revealed by real-time location data and in his movement where his location is subject to continuous tracking over an extended period of time, here thirty days," and that the Fourth Amendment requires a showing of probable cause for this information).

b. Cases Holding That Less Than Probable Cause Is Required

A minority of jurisdictions either do not recognize any protection for cell-site information, or authorize the release of information on a showing of less than probable cause. *See, e.g.*, *People v. Hall*, 14 Misc.3d 245, slip op. at 253, 257 (N.Y. Sup. Ct. 2006) (finding that the cell-phone technology at issue in the case was not a "tracking device" for purposes of the ECPA and the information was properly obtained under the SCA standard).

Although courts finding probable cause usually reject the theory that the disclosure of cell-phone information by a third party, such as a phone company, voids any privacy protection, at least a few courts taking the minority approach have employed the theory. *See, e.g.*, *United States v. Dye*, No. 1:10-CR-221, 2011 WL 1595255, at *9 (N.D. Ohio Apr. 27, 2011) ("The defendant also seeks to suppress his cell phone records, which were obtained via subpoena. However, there is no reasonable expectation of privacy in cell phone records[] or in cell-site location information."); *United States v. Benford*, No. 2:09 CR 86, 2010 WL 1266507, at *2 (N.D. Ind. Mar. 26, 2010) ("[D]efendant had no legitimate

expectation of privacy in records held by a third-party cell phone company identifying which cell phone towers communicated with defendant's cell phone at particular points in the past . . . [but] Fourth Amendment concerns might be raised if cell-site data were used to track the present movements of individuals in private locations.").

Similarly, the district court in *United States v. Suarez-Blanca*, No. 1:07-CR-0023-MHS/AJB, 2008 WL 4200156 (N.D. Ga. Apr. 21, 2008), rejected Fourth Amendment protection for historical cell-site information by combining the third-party doctrine with a finding that the defendants did not have a reasonable expectation of privacy in the location of cell phone towers. *Id.* at *8, 10; *see also In re Application of the United States for an Order* . . ., 411 F. Supp. 2d 678, 682 (W.D. La. 2006) (rejecting Fourth Amendment concerns when a "tracking" device only discloses communication with a tower and does not provide detailed tracking information regarding movement inside a private residence).

Other courts draw a sharp distinction between historical and prospective cell-site information and grant access to the former through the SCA. *See United States v. Graham*, 846 F. Supp. 2d 384, 391 (D. Md. 2012) ("*Maynard* concerned the prolonged surveillance of a vehicle by global positioning system technology, and not through historical cell-site location data. That distinction is important."). The *Graham* court concluded that individuals do not have a reasonable expectation of privacy in historical cell-site information. *See id.* at 389. But *Graham* carefully noted the distinctions between historical cell-site information and real-time GPS tracking. *See id.* at 391. Moreover, although the court rejected the proposition that the Fourth Amendment places some limits on the amount of historical cell-site information that may be obtained by the government before the search becomes

"unreasonable," the court concluded that jurisprudence was moving in that direction. *See id.* at 394. Similarly, the Third Circuit concluded, after analyzing the SCA, that probable cause is not required for the government to obtain historical cell-site information. *See In re Application of United States*, 620 F.3d 304 (3d Cir. 2010).

In many of the above cases, the government advanced a "hybrid theory" for why a showing of less than probable cause is required to obtain cell-site information. The "hybrid theory" combines the authorities of the SCA with the pen-register statute to authorize cell-site location data by reasoning that, although 47 U.S.C. § 1002(a)(2) prevents collection of location data via the pen / trap statute *alone*, the term "solely" implies that the government may acquire data when combined with an SCA request. *See generally* Stapleton at 397- 400; *In re Application for Pen Register & Trap/Trace Device with Cell Site Location Auth.*, 396 F. Supp. 2d at 761 (government argued "a pen/trap order, when combined with a § 2703(d) order, is sufficient authority to collect prospective cell site data").

4. *United States v. Skinner*

On August 14, 2012, the United States Court of Appeals for the Sixth Circuit issued *United States v. Skinner*, 690 F.3d 772 (6th Cir. 2012), holding that a criminal defendant does not have a reasonable expectation of privacy in the location data in a cell phone, and consequently that government collection of the data is not a search under the Fourth Amendment. *Id.* at 781. In *Skinner*, during an investigation into a drug trafficking ring, the government obtained an order from a magistrate judge authorizing the collection of real-time cell-site location data for a cell phone that belonged to the defendant. The defendant challenged the district court's decision to include the evidence at trial. In its ruling, the Sixth Circuit stated "[b]ecause authorities tracked a known number that was voluntarily used

while traveling on public thoroughfares, Skinner did not have a reasonable expectation of privacy in the GPS data and location of his cell phone." *Id.*

In reaching its decision, the Sixth Circuit relied directly on *Knotts*' holding that "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another." *Id.* at 778 (citing *Knotts*, 460 U.S. at 281). The court noted that "Skinner was traveling on a public road before he stopped at a public rest stop. While the cell site information aided the police in determining Skinner's location, that same information could have been obtained through visual surveillance." *Id.*

The Sixth Circuit also relied on its decision in *United States v. Forest*, in which the court determined that DEA agents' actions of dialing a suspect's telephone number and then quickly hanging up in order to obtain location data from the suspect's phone was not a search under the Fourth Amendment. *Forest*, 355 F.3d at 951 (finding "no legitimate expectation of privacy in the cell-site data because the DEA agents could have obtained the same information by following [the defendant's] car"). In *Skinner*, the court stated that *Forest* stands for the proposition that cell-site data is merely a proxy for an individual's location, and thus a defendant does not have a legitimate expectation of privacy in the data. *Skinner*, 690 F.3d at 778.

Finally, the court distinguished *United States v. Jones,* the Supreme Court's recent decision addressing use of GPS tracking devices, noting that "the DEA agents only tracked Skinner's cell phone for three days," in contrast to the "intensive monitoring over a 28-day period" that took place in *Jones*. *Id.* at 780 (quoting *Jones,* 132 S. Ct. at 957). Concluding that "[n]o such extreme comprehensive tracking is present in this case," the court found that *Skinner* did not "present the concern" raised in *Jones. Id.*

a. *Skinner* Distinguished

Although *Skinner*'s facts resemble the case here — both cases involve a major drug trafficking investigation and real-time cell-site location data tracking — *Skinner* is distinguishable for two key reasons.

First, *Skinner* is clearly different from this case with respect to the duration of the government's tracking. In *Skinner*, the DEA tracked the defendant for three days. In this case, the government secured tracking data for multiple cell phones over the course of half a year, from March 11, 2010, to roughly the end of 2010 when Defendants were arrested. Considering the phones individually, each warrant issued for a minimum of thirty or forty-five days. The *Skinner* court specifically noted that its holding dealt with "relatively short-term monitoring of a person's movements," and drew a contrast with the "intensive monitoring over a 28-day period" present in *Jones. Id.* at 780 (quoting *Jones,* 132 S. Ct. at 957). In other words, based solely on the difference between a three-day and a seven-month period of cell-site tracking, the Court finds this case *does* present the concerns regarding extreme comprehensive tracking raised in *Jones*.

Second, *Skinner* relied on the *Knotts* and *Forest* line of cases and their rationales to find that use of a tracking device *on a public thoroughfare* was permissible. *Skinner*'s holding applied to "track[ing] a known number that was voluntarily used *while traveling on public thoroughfares* . . ." *Id.* at 781 (emphasis added) (also stating "the monitoring of the location of the contraband-carrying vehicle *as it crossed the country* is no more of a comprehensively invasive search than if the car was identified in Arizona and then *tracked visually* . . . as the vehicles progressed"). This basis for distinguishing the instant case from *Skinner* is related to the first. It is true that the functional impact on privacy of a police

officer following a suspect on a highway in an unmarked police car, or using cell-phone technology to do the same, is minimal. And it appears that the agents in *Skinner* collected cell-site location data only while the suspect was on public thoroughfares. Here, however, real-time cell-site location data was collected for more than half a year. The government concedes, and DEA Special Agent Edward Donovan's testimony and the affidavits on file confirm, that the cell phones were tracked for a significant amount of time during the investigation. *See* June 17 Donovan Aff. at ¶ 64, ECF No. 74-7; Hr'g I at 33. Given the duration and intensity of the tracking, it cannot be reasonably argued that *only* public-thoroughfare data was collected. The government certainly collected cell-site data emanating from within the defendants' homes or from another place in which the defendants had a legitimate expectation of privacy.

At this point, the analogy between cell-phone tracking and visual surveillance breaks down. In *United States v. Karo*, 468 U.S. 705 (1984), the Supreme Court considered, as a follow-up to *Knotts*, the use of a beeper to track an object's movement from a public highway to the inside of a residence. The Court noted that although a DEA agent may physically track a suspect on a public road, and by analogy may use a beeper to do the same,

> had a DEA agent thought it useful . . . 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.

Id. at 715. The distinction is clear: the government may use a beeper to track location in public areas, but may not do so when tracking continues into a protected area, such as a residence, without a warrant.

Based on these distinctions, the Court finds that the issues in *Skinner* are distinguishable from the issues presented in this case: long-term cell-phone tracking into protected areas.

C. Conclusion and Findings of Law

After a careful review of the statutes and decisions set forth above, the Court makes the following findings.

1. Fourth Amendment Implications

First, the public-thoroughfare distinction employed in *Knotts* and *Skinner* does not fully address all legal issues presented when, as here, the government seeks to acquire real-time cell-site location data for prospective periods as long as thirty-to-forty-five days or more — tracking for a period of time long enough to monitor an individual in a protected area. *Skinner* explicitly stated that *Jones* does not limit or overrule *Knotts* or *Karo*. *Skinner*, 690 F.3d at 779-780. But *Karo's* holding was not founded entirely on physical trespass; rather, the illegality in that case stemmed from the "*monitoring* of the beeper." *Karo*, 468 U.S. at 713. Information regarding the beeper's location inside a private residence would only otherwise have been obtainable by a search of that residence; that is, a police officer would have to, in some manner, enter the premises to obtain the information generated by the beeper. Absent a warrant, the entry would be unconstitutional. The same focus underlies the Court's concern here. If at any point a tracked cell phone signaled that it was inside a private residence (or other location protected by the Fourth Amendment), the only

other way for the government to have obtained that information would be by entry into the protected area, which the government could not do without a warrant.

The Court's concern here was addressed by the Supreme Court in *Kyllo v. United States*, 533 U.S. 27 (2001), which upheld the general principle that the use of technology was a search when used to collect information that otherwise could not have been obtained without a physical search. *See Id.* at 31. In *Kyllo*, the police used a thermal imaging device to determine whether the suspect's home was radiating an abnormally high amount of heat. The Court concluded that, as in *Karo*, the only way police could otherwise have obtained the information provided by the device would have been by a search inside the home. *Id.* In these situations, which are well beyond the facts analyzed by the court in *Skinner*, a warrant would be required.[6]

Kyllo raised another issue implicated by real-time cell-site tracking warrants. In *Kyllo*, the Court rejected the argument that the government could restrict its thermal searches to non-"intimate" details based on the practical observation that "[n]o police officer would be able to know *in advance* whether his through-the-wall surveillance picks up 'intimate' details–and thus would be unable to know in advance whether it is Constitutional." *Id*. at 38 (italics added). The same problem is posed by requests for prospective real-time cell-

[6] *See also Florida v. Jardines*, 133 S. Ct. 1409 (2013). In *Jardines*, the Supreme Court found that the use of a drug-sniffing dog within the curtilage of a defendant's home constituted a search because of the government physically trespassed with the dog onto a protected area without permission. *Id.* at 1415 ("the only question is whether [defendant] had given his leave (even implicitly) for [the police and dog to enter the curtilage]. He had not."). The concurrence, citing *Kyllo*, would have found that use of a drug-sniffing dog invaded the defendant's reasonable expectation of privacy: the police "conducted a search because they used a device . . . not in general public use (a trained police dog) to explore details of the home (the presence of [drugs]) that they would not otherwise have discovered without entering the premises." *Id.* at 1419 (Kagan, J., concurring) (internal quotation marks omitted).

site location data. The March 11, 2010 warrant authorized the DEA to collect real-time cell-site location data for up to thirty days. Under virtually any circumstance, there was no way the DEA could *know in advance* whether or not the location data collected during that period would come from within a protected area.

Special Agent Donovan stated that the same day that he secured the warrant here, he began to "chase" the phone by pinging it and receiving location information. Hr'g I at 87. Although the information led Donovan to a suspect driving a truck, he could not have known in advance that the phone would not instead have been pinged in a suspect's bedroom. *See also In re Application of United States for an Order Authorizing Disclosure of Location Information*, 849 F. Supp. 2d at 538 ("[I]t is impossible for law enforcement agents to determine prior to obtaining real-time location data whether doing so infringes upon the subject's reasonable expectation of privacy and therefore constitutes a Fourth Amendment search."); *In re Application of U.S. for an Order Authorizing Installation & Use of a Pen Register & a Caller Identification Sys. on Tel. Numbers (Sealed)*, 402 F. Supp. 2d 597, 605 (D. Md. 2005) ("To the extent the government seeks to act without a warrant, the government acts at its peril, as it may not monitor an electronic tracking device in a private place without a warrant.").

The Court's Fourth Amendment concerns also overlap with those expressed by the D.C. Circuit in *Maynard*, and in the *Jones* concurrences. *See Maynard*, 615 F.3d at 562; *Jones*, 132 S. Ct. at 963-64 (Alito J., concurring in the judgment); *Jones*, 132 S. Ct. at 954-57 (Sotomayor, J., concurring). Generally speaking, those opinions express the view that warrantless long-term tracking by electronic means violates an individual's reasonable expectation of privacy, not just because of the potential for tracking into protected areas,

because the information obtained through such means is, in the aggregate, so comprehensive.[7] *See, e.g.*, *Jones*, 132 S. Ct. at 964 ("[S]ociety's expectation has been that law enforcement agents and others would not — and indeed, in the main, simply could not — secretly monitor and catalogue every single movement of an individual's car for a very long period.") (Alito, J., concurring). The *Jones* majority found the Fourth Amendment implicated on narrower, property-based grounds, and declined to decide whether surveillance of Jones over thirty days by "electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy." *Id.* at 954 ("[T]he present case does not require us to answer that question."). That basis of decision is not available in this case because no device was installed, and yet the privacy concerns implicated by the tracking seem just as profound.

For these reasons, the Court finds that when the government requests authorization to engage in long-term, real-time tracking of an individual's movements via his or her cell phone, the situation reaches past the law set forth in *Skinner*, and Fourth Amendment concerns are implicated.

2. Statutory Analysis

It is also apparent that the statutory authority relevant to pen-register / trap-and-trace devices, stored communications, tracking devices, and wiretaps is not applicable to cell-phone tracking.

---

[7] This view has its critics. *See, e.g.*, Orin Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 Mich. L. Rev. 311 (2012). The present Order does not adopt any of the "mosaic theory" approaches specifically, nor does it purport to address the questions raised in Kerr's article regarding the implications of the approach. The Court simply notes that the constitutionality of long-term cell-phone tracking was left open in *Jones*, submits that the privacy issues presented by such tracking merit a doctrinal response, and finds that the facts presented here fall on the wrong side of the constitutional divide.

First, the information sought here is clearly location data and the government therefore cannot acquire it solely on the authority of the pen / trap statute, 47 U.S.C. § 1002(a)(2). *See generally In re Application of U.S. for Order*, 497 F. Supp. 2d 301, 307 (D.P.R. 2007). And neither can, as the government argued in its warrant application, law enforcement acquire real-time location information under the "hybrid" theory combining pen / trap statute and the SCA authorities. *See* March 11 Donovan Aff., ECF No. 106-1; *see also, e.g.*, *In re U.S. for Orders Authorizing Installation & Use of Pen Registers & Caller Identification Devices on Tel. Numbers*, 416 F. Supp. 2d 390, 395 (D. Md. 2006); *In re U.S. For an Order Authorizing the Disclosure of Prospective Cell Site Info.*, 412 F. Supp. 2d 947, 958 (E.D. Wis. 2006) *aff'd*, 06-MISC-004, 2006 WL 2871743 (E.D. Wis. Oct. 6, 2006).

Moreover, a cell phone is not a "tracking device" as defined by 18 U.S.C. § 3117. First, a cell phone is not a government-owned-and-installed device. Instead, it is a personal communications device that an individual purchases and owns. The statutory language of § 3117 specifically contemplates government installation: "[i]f a court is empowered to issue a warrant or other order for the *installation* of a mobile tracking device . . ." 18 U.S.C. § 3117(a); *see generally In re Application of the United States for an Order . . .*, 411 F. Supp. 2d at 681 ("Tracking devices are devices that are 'installed' at the request of the Government."). Second, the combination of tracking movement and the actual seizure (no matter how limited) of information generated by a non-government device is sufficient to consider real-time cell-site location data tracking distinct from a § 3117 authorized tracking device. Third, significant technological differences exist between tracking cell phones and tracking with § 3117 "tracking devices." There are practical limits on where a GPS tracking device attached a person's vehicle may go. A cell phone, on the other hand, is usually

carried with a person *wherever* they go. *See generally In re Application for an Order Authorizing The Extension & Use of a Pen Register Device*, 07-SW-034-GGH, 2007 WL 397129, at *2 (E.D. Cal. Feb. 1, 2007) ("[I]t would prove far too much to find that Congress contemplated legislating about cell phones as tracking devices."). Because a cell phone is not a "tracking device" under § 3117, the procedure set forth in Criminal Rule 41 for the installation and use of "tracking devices" is also not applicable to the acquisition of real-time cell-site location data. *See* Fed. R. Crim. P. 41(a)(2)(E) (providing that "tracking device," as used in that rule, "has the meaning set out in 18 U.S.C. § 3117(b)").

Third, there is cause for a firm distinction between historic location data, and live, real-time location data that enables real-time location monitoring. *See, e.g.*, *In re Applications of United States for Orders Pursuant to Title 18, U.S. Code Section 2703(d)*, 509 F. Supp. 2d 76, 78 (D. Mass. 2007) (drawing distinction between government acquisition of real-time and historic location information). Although many of the privacy questions, particularly those concerned with government compilation of a record of a person's movements, *see Skinner*, 690 F.3d at 780, are the same in historic and prospective tracking cases, the issue presented here is an application for government acquisition of real-time cell-site location data far into the future. Accordingly, this order does not address applications and authorizations for data that is "historic" or obtained as stored communications for the purposes of the SCA.

Finally, real-time cell-site location data are also not "communications" subject to Title III's heightened procedures for intercepting communications via wiretap. While information regarding an individual's location is a "communication" in some sense of the term, so are the numbers dialed in and out of a telephone. In either case, however, that location

information is not the "content" of actual communications intended to be protected by Title III wiretapping authority. *See generally In re Application for Pen Register and Trap/Trace Device with Cell-site Location Authority*, 396 F. Supp. 2d at 758 ("Cell site data does not reflect the 'contents' of a communication as that term is defined by the Wiretap Act.").

3. Probable Cause Showing for Real-Time Cell-Phone Tracking

In the absence of a definitive statutory niche for prospective cell-phone tracking, and in light of the considerable, and distinctive, privacy concerns raised by long-term, real-time cell-site tracking discussed above, scrutiny of the appropriate probable-cause showing in these cases is called for. The Court concludes that a specific showing is required to establish probable cause when the government seeks a warrant for long-term real-time tracking of an individual via a cell phone. Such a showing should include facts supporting, at least, the following:

First, that the actual location of the person the government intends to track via the cell phone is relevant to the investigation of the ongoing crime, or evidence sought. That is, if the government intends to track an individual over a long period of time, and cannot show that the individual will be, for example, in public, non-protected locations for the duration of the tracking, then the warrant application should set forth facts that warrant intrusion into protected locations that the individual may frequent. In other words, the government should set forth a probable-cause basis for following the individual into protected areas via the individual's personal cell phone.

It is true that, in a sense, a person's location is in some way *always* relevant to his potential participation in a crime. And, a person does not have a general privacy interest in his location. But before the government may use an individual's cell phone to track him

into areas in which an individual *does* have a reasonable expectation of privacy, the government should show more than that the person is suspected of a crime; the government should show that the person's location in the protected area is in some way relevant to the ongoing investigation of criminal activity. *See generally United States v. Frazier*, 423 F.3d 526, 532 (6th Cir. 2005) ("The critical element in a reasonable search is not that the owner of property is suspected of crime but that there is reasonable cause to believe that the specific 'things' to be searched for and seized are located on the property to which entry is sought").

Second, the government should show that the specific *cell phone*, as well as the person to be tracked, is relevant to the investigation. That is, the government must show there is a nexus between the cell phone, the suspect, and the information sought. *See generally United States v. Carpenter*, 360 F.3d 591, 594 (6th Cir. 2004) (warrant application must show "a nexus between the place to be searched and the evidence to be sought"); *see also, e.g.*, *United States v. Sierra-Rodriguez*, 10-20338, 2012 WL 1199599, at *6 (E.D. Mich. Apr. 10, 2012) (finding probable cause shown where the affidavit provided substantial basis to conclude that specific cell phone tracked belonged to suspect embarking on criminally-related travel). This means that the government should show that a criminal suspect under investigation is the likely user of the cell phone at issue and that he or she uses the cell phone in connection with criminal activity. Investigation of a criminal organization using multiple phones, including dedicated phones for criminal activity, over the course of the operation would require the government to make a showing as to each phone it intends to track. The logic of this requirement is simply that, drawing on the Fourth Amendment's particularity requirement, tracking a phone used in furtherance of criminal

activity is likely to lead to evidence of criminal activity, whereas tracking phones, the use of which is unconnected to criminal activity, will likely demonstrate where a person conducts highly personal business.

In sum, because "the belief that the items sought will be found at the location to be searched must be supported by less than prima facie proof but more than mere suspicion," to establish probable cause for long-term, real-time, cell-site tracking, the government should have to demonstrate a nexus between a suspect and the phone, the phone and the criminal activity, as well as the criminal activity and suspect's location in protected areas, rather than merely probable cause that the person is engaged in criminal activity. *See generally United States v. Williams*, 544 F.3d 683, 686 (6th Cir. 2008).

This standard obviously does not deal a serious blow to the government's ability to obtain real-time cell-site location data. Although specific, the showings required are nowhere near as stringent as those for a Title III wiretap, which require agents to state that "normal investigative procedures have been tried and failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous" by including "a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous." *United States v. Poulsen*, 655 F.3d 492, 503 (6th Cir. 2011), *reh'g denied* (Oct. 17, 2011), *cert. denied*, 132 S. Ct. 1772, 1182 (2012) (quoting *United States v. Rice*, 478 F.3d 704, 716 (6th Cir. 2007)). The showing described here does not require exhaustion of other investigative techniques; it simply calls for the government to provide additional facts in its warrant application to justify tracking an individual via his personal cell phone, over an extended period of time, into protected spaces. The result is a showing that is not

necessarily *heightened*, rather it is simply responsive to the full range of recognized privacy interests at stake in long-term cell-phone tracking.

Of course, any warrant requirement exacts some costs on the ability of police to investigate crimes. But "[a]n essential purpose of a warrant requirement is to protect privacy interests by assuring citizens subject to a search or seizure that such intrusions are not the random or arbitrary acts of government agents." *United States v. Rohrig*, 98 F.3d 1506, 1514 (6th Cir. 1996) (quoting *Skinner v. Railway Labor Executives' Ass'n*, 489 U.S. 602, 621-22 (1989)). The tailored showing described here would help prevent the arbitrary or casual invasion of privacy rights that technological change facilitates. This is a significant concern for modern Fourth Amendment jurisprudence, as recognized in *Jones*. *See Jones*,132 S. Ct. at 963 (Alito, J. concurring in judgment) (noting that privacy protections were greater in "the pre-computer age," because "[t]raditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken"). In practical terms, the consequences of requiring a tailored showing in this instance might be no more than that the government would seek cell-site data for a shorter duration, or would invest more time in physical surveillance to gather necessary facts prior to seeking a warrant.

It is true that other courts usually do not require the showing discussed here and no authoritative court has stated plainly that such a showing is required. It is also true that in certain cases, there is no practical difference between obtaining a warrant to use technology to track a suspect and simply using traditional means to do it; the government can often detail DEA agents to follow suspects on highways for a few hours almost as easily as they can track a cell phone. But the same technology and grant of authority, without more care, can also permit the government to conduct near-limitless around-the-

clock surveillance of a person's location, subject only to the limitation of where the suspect may not have taken a cell phone. As discussed with concern in *Skinner* and *Jones*, such 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." *Jones*, 132 S. Ct. at 955 (Sotomayor, J. concurring) (quoting *People v. Weaver*, 12 N.Y.3d 433, 441-442 (2009)). To date, real-time cell-phone location-data tracking is the easiest means to gather the most comprehensive data about a person's public — and *private* — movements available. The standard discussed here is responsive to this concern, and is not inconsistent with the precedent that binds this Court.

4. Limitations of the Standard

The cell-phone tracking standard is meant to be read in harmony with the Sixth Circuit's holding in *Skinner.* Specifically, if the government seeks to track an individual for a short period of time only, with no foreseeable intrusion into protected areas, the probable-cause showing discussed here would not apply and *Skinner* would plainly govern. If, for example, the tracking was to be done for a limited purpose on public thoroughfares — like in *Skinner*, with foreknowledge a suspect was taking a two day cross-country trip — the specific Fourth Amendment concerns addressed here would not be raised. But if the tracking the government seeks to undertake is similar to the "intensive 28-day" monitoring the Sixth Circuit itself distinguished, then the more detailed showing required to meet the cell-phone tracking standard should be made.

Applying the cell-phone tracking standard to this case, the Court finds, as discussed next, that the government did not make the necessary probable-cause showing in the March 11, 2010 warrant application.

D. Probable Cause for the March 11, 2010 Warrant

To obtain the real-time cell-site location data for the challenged phones, the government obtained the previously mentioned Criminal Rule 41 probable-cause warrant for each phone. Strictly speaking, Defendants challenge all of the search warrants for cell-site and GPS location data, but their primary argument is that the first March 11, 2010 search warrant was not supported by probable cause and the remaining warrants are the "fruit of the poisonous tree" of that original warrant.[8]

For a warrant to issue, a magistrate judge must find probable cause such that there is a "fair probability . . . that contraband or evidence of a crime will be found in a particular place." *United States v. Gardiner*, 463 F.3d 445, 470 (6th Cir. 2006) (quoting *United States v. Davidson*, 936 F.2d 856, 859 (6th Cir. 1991)). A magistrate judge need only find that there are "reasonable grounds for belief" that evidence will be found. *Id.* Probable cause is assessed on review of the "four corners" of the affidavit submitted to the magistrate judge, and usually not from extrinsic evidence introduced later. *Frazier*, 423 F.3d at 535. Once a magistrate judge has decided that probable cause exists, as long as the magistrate judge had a "substantial basis" for that conclusion, a reviewing court should uphold the order. *Gardiner*, 463 F.3d at 470. When, as here, an affidavit by a law enforcement officer is the basis for the magistrate judge's opinion, the affidavit itself must provide "a substantial basis for determining the existence of probable cause." *Id.* Search warrant affidavits are judged on the totality of the circumstances, not by line-by-line scrutiny. *See generally United States v. Woosley*, 361 F.3d 924, 926 (6th Cir. 2004).

---

[8] Defendants also challenge the October 5, 2010 warrant as derivative of the Whigham vehicle search. Because the Court will admit all the evidence seized during the Whigham vehicle search, discussed *infra*, at 39, the Court will not consider this challenge any further.

1. Summary of the March 11, 2010 Donovan Affidavit

Defendants first challenge the probable-cause basis for the search warrant for cell-phone number (313) 529-5848, subscribed to by Carlos Powell. DEA Special Agent Edward Donovan prepared the affidavit in support of the March 11, 2010 application. *See* March 11, 2011 Search Warrant App., ECF No. 106-1. Magistrate Judge Donald Scheer approved the application.

In the affidavit, Donovan stated the following: He and other DEA agents were investigating a large-scale drug-trafficking ring between Arizona, Illinois, and Michigan. During the course of the investigation, Ted Morawa was arrested and indicted in federal district court in Arizona. Mar. 11 Donovan Aff. at ¶ 7. Morawa agreed to cooperate and proffered that part of the drug trafficking ring involved him delivering or causing to be delivered over 200 kilograms of cocaine and over 100 kilograms of heroin to an individual in Detroit, Michigan then only known as "50," and subsequently identified by Morawa as Defendant Carlos Powell. Based on Morawa's direct statements and proffers, and evidence supporting the veracity of Morawa's statements in the form of intercepted communications, money seizures, and drug seizures, Donovan believed Morawa to be a credible source. *Id*. at ¶¶ 8, 10.

Separately, agents of the Detroit DEA and Detroit Internal Revenue Service Criminal Investigation Division interviewed a cooperating defendant witness, the owner and operator of a jewelry store in Detroit. The cooperating defendant witness stated that defendant Carlos Powell purchased several hundreds of thousands of dollars worth of jewelry in cash from the store. *Id.* at ¶ 12. Donovan stated that, in his education and experience, such purchases in cash were often derived from the sale of narcotics. *Id.* at ¶ 13.

Donovan learned that the T-Mobile cell phone number (313) 529-5848 was subscribed to by Carlos Powell, who at the time was identified as residing at 16475 Ego Avenue, Eastpointe, Michigan. Donovan and other agents attempted to locate Carlos Powell, Carlos Powell's vehicles, or other residences frequented by Carlos Powell, but had no success. *Id*. at ¶ 15. Donovan stated he believed that requesting the GPS location data related to (313) 529-5848 would assist with tracking Carlos Powell, identifying locations used by Carlos Powell to store narcotics, identifying Carlos Powell's associates, and identifying Carlos Powell's assets derived from unlawful narcotics sales. *Id*.

Magistrate Judge Scheer granted the application on March 11, 2010, and ordered the cell-phone service provider to provide all assistance necessary to ascertain the physical location of the cell phone associated with the number (313) 529-5848, for a period of thirty days. The magistrate judge found probable cause to believe the information would lead to evidence of violations of the drug code, as well as the identification of such violators. *See* Mar. 11 Warrant, ECF No. 106-1 at 13.

2. Probable Cause Analysis

Defendants argue that the March 11 Donovan Affidavit was insufficient to provide a substantial basis for the magistrate judge to find probable cause to issue the warrant. Defendants state that the affidavit provided "even less of a showing of probable cause" than subsequent warrants which themselves were "deficient." Supp. Mem. at 1, ECF No. 106. Defendants argue that the affidavit put forth no evidence that the (313) 529-5848 telephone was used in connection with any unlawful activity. Likewise, Defendants note that the information provided by Morawa was not dated, and therefore did not establish

probable cause that Carlos Powell was engaged in illegal activity at the time the warrant was sought.

In response, the government submits that the affidavit was more than sufficient to show probable cause and that it afforded the magistrate judge a substantial basis on which to grant the warrant. The government argues that the affidavit clearly established through both informant testimony and independent verification the likelihood that Carlos Powell was a major drug trafficker in Detroit. The government also argues that the testimony established Carlos Powell as an active drug dealer, and that the information was not stale. Moreover, it argues that the DEA was entitled to rely on the search warrant under the good faith exception.

After reviewing the March 11 Donovan Affidavit, the Court concludes that the affidavit provided, under traditional probable cause analysis, a sufficient basis for the magistrate judge to find probable cause to issue the warrant. The core of the affidavit was the informant testimony, confirmed by independently verified evidence, that Carlos Powell was a major player in a drug trafficking ring in Detroit. Although the affidavit relied to some extent on hearsay, it was corroborated by independently obtained evidence that permitted Donovan to make a reasonable conclusion that Morawa's statements were true. And, in any event, a police officer may rely on hearsay from an informant to establish probable cause, even for warrantless searches, "so long as the informant's statement is reasonably corroborated by other matters within the officer's knowledge." *United States v. Helton*, 314 F.3d 812, 819 (6th Cir. 2003) (quoting *Jones v. United States*, 362 U.S. 257, 269-70 (1960)). Donovan found Morawa reliable based on Morawa's statements *and* additional corroborating evidence from the investigation that supported Morawa's statements. *See*

Mar. 11 Donovan Aff. at ¶ 8. Accordingly, the Court finds that under the prevailing probable-cause standard, a substantial basis existed to find probable cause that Carlos Powell was a drug dealer and that tracking his cell phone would lead to evidence of a crime. *See, e.g.*, *United States v. Medina-Meraz*, No. 10-20338, 2012 WL 1364612, at *3 (E.D. Mich. Apr. 19, 2012).

The affidavit does not make a sufficient showing to establish probable cause, however, under the cell-phone tracking standard discussed above. Although it does state sufficient facts to demonstrate that Powell was involved in a large-scale drug trafficking organization, and that the cell phone to be tracked belonged to Powell, it did not set forth facts to demonstrate a nexus between the cell phone and the criminal activity, or between Powell's location in protected areas and the criminal activity. First, although the affidavit states that Morawa communicated with Powell in furtherance of the narcotics trafficking, it does not state that Morawa and Powell communicated by cell phone, or that Morawa contacted Powell at the specific cell-phone number at issue here. Second, the affidavit sought cell-phone location data to determine Powell's location, but it also sought to track the phone for a period of 45 days — significantly longer than reasonably necessary to determine Powell's location. And the tracking was unquestionably long enough to trigger the concern that agents would track Powell's location in protected areas, like his residence. The affidavit does not set forth any facts to support a finding that tracking Powell via his cell phone into, for example, his residence, would lead to evidence of the suspected criminal activity. Accordingly, the Court finds the affidavit does not establish probable cause sufficient to warrant the invasion of privacy brought about by long-term real-time cell phone tracking. A reasonable alternative procedure that the government could have followed in

this instance would have been to seek short-term cell-phone location data for the limited purpose of determining Powell's location. The government could then have dispatched agents to track Powell physically until they uncovered the additional facts necessary to show a nexus between any protected locations frequented by Powell and the suspected criminal activity. Armed with those facts, the government would readily have met the cell-phone tracking standard described here.

3. Good Faith Exception

Under the Court's construction of the applicable precedent, the government did not make a sufficient showing to demonstrate that probable cause existed for the warrant to issue. The evidence is nonetheless admissible, however, because whether or not the warrant issued on probable cause, the government relied on it in good faith. *See Buford*, 632 F.3d at 271 ("[S]uppression is not an available remedy when police officers conducted a search in good faith reliance on some higher authority, such as a warrant or a statute, even if the warrant or statute were later held invalid or unconstitutional (the 'good faith exception')."") (citation omitted).

The exception is not absolute. The Supreme Court has outlined four scenarios when good-faith reliance on a warrant is not sufficient: "(1) when the warrant is issued on the basis of an affidavit that the affiant knows (or is reckless in not knowing) contains false information; (2) when the issuing magistrate abandons his neutral and detached role and serves as a rubber stamp for police activities; (3) when the affidavit is so lacking in indicia of probable cause that a belief in its existence is objectively unreasonable; and, (4) when the warrant is so facially deficient that it cannot reasonably be presumed to be valid." *United States v. Leon*, 468 U.S. 897, 914 (1984)).

Defendants argue that the exception does not apply here because the affidavit is lacking in indicia of probable cause, such that the DEA's reliance on it was objectively unreasonable. An affidavit is lacking in indicia of probable cause, also known as a "bare bones" affidavit, if it contains only "suspicions, beliefs, or conclusions, without providing some underlying factual circumstances regarding veracity, reliability, and basis of knowledge." *United States v. Laughton*, 409 F.3d 744, 748-49 (6th Cir. 2005) (quoting *United States v. Weaver*, 99 F.3d 1372, 1378 (6th Cir. 1996)). This standard is "a less demanding showing than the 'substantial basis' threshold required to prove the existence of probable cause in the first place." *Id.* (quoting *Carpenter*, 360 F.3d at 595). The Court has already found that the affidavit met the substantial-basis threshold; it necessarily was also not lacking in indicia of probable cause. Accordingly, the good-faith exception applies. The evidence obtained pursuant to the March 11, 2010 warrant for real-time cell-site location data is admissible and will not be suppressed.

E. "Fruit of the Poisonous Tree" and the Remaining Cell-Site Warrants

Defendants argue that if the initial March 11, 2010 search was unreasonable, any evidence obtained from it — specifically the subsequent real-time cell-site location-data search warrants — are "fruit of the poisonous tree" and are therefore inadmissible. Defendants are correct that when the government exploits illegally obtained evidence, subsequent searches and seizures based on that evidence are tainted and subject to the exclusionary rule. *See Pearce*, 531 F.3d at 381(citing *Wong Sun*, 371 U.S. at 484-85). But because all the evidence obtained pursuant to the March 11, 2010 warrant is admissible under the good-faith exception, the remaining warrants are, therefore, not based on any tainted material that would justify suppression under the derivative rule. Moreover, having

reviewed the affidavits submitted in support of each warrant, the Court also finds that the government obtained the warrants from a neutral and detached magistrate judge based on more than a "bare bones" affidavit, and that therefore, the evidence obtained from the subsequent warrants is also admissible under the good-faith exception.

III. Warrantless Use of GPS Tracking Devices / Vehicle Searches

Next, Defendants challenge the government's warrantless installation of GPS tracking devices on vehicles belonging to Carlos Powell[9] and Eric Powell, and the use of the location data obtained to conduct four traffic stops in which evidence was seized.[10] As set forth below, the Court concludes that whether or not the installation and use of the GPS devices was an unconstitutional search, the evidence seized in the traffic stops is admissible under exceptions to the exclusionary rule. The Court will first discuss the use of the GPS tracking devices, and then discuss the traffic stops.

A. GPS Tracking Device

As stated above, the Court conducted an evidentiary hearing on January 17 and February 12, 2013 to provide a factual basis for a decision on the motion to suppress. Special Agent Donovan was the only witness. He testified regarding his and the DEA's

[9] Special Agent Donovan testified that the government did not collect or use any data from the tracking device affixed to Carlos Powell's car. Hr'g I at 17-18. Because there is no evidence to suppress from the use of that tracking device, the Court will discuss only the tracking device affixed to Eric Powell's vehicle.

[10] In addition to their fruit-of-the poisonous-tree objection to the evidence seized in the traffic stops, Defendants also seek to directly suppress the location data seized from the GPS tracker. The location-data evidence, strictly speaking, is simply evidence of the location of Eric Powell's truck at any given moment. As a practical matter, therefore, suppression of the GPS data regarding the location of Powell's truck, without anything more, really suppresses nothing. Moreover, the uncontroversial DEA testimony that Powell's truck was on a highway on any particular day, would be permissible in any event, given the extensive in-person police presence on the highways, as discussed below.

actions in using the GPS tracker to follow Eric Powell's vehicle during the investigation. *See* Hr'g I at 15. The following facts are taken from his testimony.

1. Technical Background

The DEA used a GPS tracker that affixes to the undercarriage or other unobtrusive spot on a vehicle. The tracker is "self-contained," and is found within a storage box that protects it from the elements. The box is attached with magnets to the undercarriage of a vehicle. *Id.* at 16. The GPS unit transmits its coordinates via the internet. During a typical operation, a DEA or other federal agent has a laptop computer with a wireless internet connection. At any time, the DEA agent can "ping" the GPS tracker by pressing a button on the tracking program. The GPS tracker then transmits its coordinates back to the computer. The program can ping a tracker at regular intervals as long as half an hour or as short as every minute, or whenever the agent wishes. *Id.* at 53; Hr'g II. There can be a time delay of up to ten minutes between when the GPS tracker transmits its coordinates and when the DEA agent receives the coordinates on the computer. Hr'g I at 54. The printed records of the location data show only when the data was generated, and not when a DEA agent accessed or received the data. Hr'g II. The GPS tracking device is generally accurate to within several meters, and the location data will state the variation from the coordinate reading. For example, a 12-meter variation and a direction would indicate that the actual GPS unit could be within 12 meters from the coordinate reading. *Id.*

The location data is stored on a remote computer server, capable of being accessed by the DEA, and it is usually archived. Hr'g II. On cross-examination, Donovan testified that archived location data for the first two months of the tracking, beginning around June 10, 2010, was inadvertently lost. Typically, the servers keep the data for several months. In this

case, the servers overwrote the data as part of an apparently normal record storage procedure. The first available tracking records begin on or around August 31, 2010. *Id.*

2. GPS Tracker Installation and Re-Installation

Before placing the GPS tracking device on Eric Powell's truck, the DEA had amassed considerable evidence about the overall drug trafficking ring and Eric Powell's involvement in it. On approximately June 10, 2010, the DEA located Eric Powell's Chevy Silverado pick-up truck parked in the driveway of Eric Powell's residence at 24505 Franklin Farms Drive, in Franklin, Michigan. Hr'g I at 19-21.The DEA changed out the battery on the tracking devices several times. Most of the time, the change-out was done in Eric Powell's driveway. On three occasions, the truck was parked elsewhere: in front of Earnest Proge's residence, in the commercial parking lot of a warehouse, and in the parking lot of a car dealership. *Id.* at 21-22.

Powell's home is in a gated community. A security gate blocked the entrance to Franklin Farms Drive, and on the gate there was a sign reading "private property, no trespassing." To install the GPS device, the DEA agents simply walked around the gate, as it is only a vehicular gate and does not bar foot traffic. Hr'g II. During daylight hours, Donovan has driven to the gate and it has opened automatically. *Id.* Donovan installed the GPS tracker at night, and is unsure whether or not the gate would have opened automatically at that time. *Id.*

3. Constitutionality of the GPS tracker

Defendants principally challenge the use of the GPS trackers under *Jones*, arguing that after *Jones*, "it seems clear enough that the warrantless employment of the tracking devices constituted a Fourth Amendment violation." Mot. to Dismiss at 2. Defendants also

argue that whether or not the warrantless installation of the GPS devices was itself a Fourth Amendment violation under *Jones*, the long-term use of the GPS device to track Powell's vehicle moves the surveillance beyond the realm of a reasonable search and into one that was clearly unreasonable. Finally, Defendants argue that because Powell's truck was parked in a gated community, requiring key-card access to enter, the DEA agents committed a standard trespass, and hence an unconstitutional search, by entering the property to plant the GPS device. Hr'g II.

Taking the last argument first, it is true that gated communities are "private property" in the general sense and are designed to restrict access to the community. But it is not true that residence in a gated community transforms the entire community into an individual's private property for Fourth Amendment purposes. *See United States v. Harris*, 6 F. App'x 304, 308 (6th Cir. 2001) (holding that the "curtilage" and "public areas" doctrines do not apply differently to gated communities than to regular neighborhoods). Here, as in *Harris*, Powell's gated community is not his exclusive property such that the agents could violate Powell's reasonable expectation of privacy by entering. As *Harris* noted, "other residents and their guests, garbage collectors, and other service providers" have regular access to the community. *See id*.

With respect to *Jones*, the parties disagree about the scope of its holding. In that case, police installed a GPS device on a vehicle and used the data collected to monitor the defendant's movements for four weeks. The Supreme Court held that the physical installation of the GPS device was a "search" under the Fourth Amendment and affirmed the court of appeals' finding that evidence obtained as a result should have been excluded at trial. *Jones*, 132 S. Ct. at 949. Defendants argue that *Jones* holds that the warrantless

installation of a GPS tracker is an *unreasonable* search to which the exclusionary rule always applies, or at least that the search was unreasonable here. The government argues that *Jones* holds simply that installation of the device is a Fourth Amendment search, and leaves open the question of whether or not such a search could be reasonable. In the instant case, the government contends, the search was reasonable. The Court will not reach the issue, because, for the reasons explained next, all the evidence seized in the traffic stops would be admissible even if the installation and use of the GPS tracker was an unreasonable search otherwise subject to the exclusionary rule.[11]

B. The Traffic Stops

Defendants seek suppression of evidence seized during four traffic stops. Specifically, Defendants argue that installation of the GPS device on Powell's car allowed police to seize evidence in vehicle searches during: (1) the June 23, 2010 traffic stop and search of Benny Whigham's vehicle; (2) the September 17, 2010 traffic stop of Earnest Proge's vehicle; (3) the June 28, 2010 traffic stop and search of Juan Valle's vehicle; and (4) the October 22, 2010 traffic stop and search of Margarita de Vallejo's vehicle. The Court finds that the evidence seized in the traffic stops is admissible because each stop falls within an exception to the exclusionary rule.

1. Legal Standards

A police officer may lawfully stop a car if there is "probable cause to believe that a civil traffic violation has occurred, or reasonable suspicion of an ongoing crime." *United States*

[11] Nor will the Court discuss the government's arguments that the officers' good-faith reliance on the existing law pre-*Jones* provides an exception to application of the exclusionary rule in this case. *See Davis v. United States*, 131 S. Ct. 2419, 2429 (2011) ("Evidence obtained during a search conducted in reasonable reliance on binding precedent is not subject to the exclusionary rule.").

v. Blair, 524 F.3d 740, 748 (6th Cir. 2008) (citations and internal quotation marks omitted). A traffic stop is a "seizure" within the meaning of the Fourth Amendment, and evidence seized during an illegal stop "must be suppressed as fruits of the poisonous tree." *United States v. Jackson*, 682 F.3d 448, 453 (6th Cir. 2012) *cert. denied*, 133 S. Ct. 370 (2012). Defendants argue that the traffic stops at issue here were illegal as the fruit of the poisonous tree of the installation and use of the GPS tracker.[12]

Three exceptions to the exclusionary rule permit the admission of evidence, even when a Fourth Amendment violation has occurred: the independent-source, inevitable-discovery, and attenuation doctrines. *See generally United States v. Kennedy*, 61 F.3d 494, 497 (6th Cir. 1995). The independent-source doctrine states that even if an illegal search occurs during an investigation, if "a proper, independent search led to the evidence in question," then the evidence may still be admitted. *United States v. Baldwin*, 114 F. App'x 675, 681 (6th Cir. 2004) (quoting *United States v. Dice*, 200 F.3d 978, 984 (6th Cir. 2000)).

Similarly, under the inevitable-discovery doctrine, evidence is admissible if the government proves that it "inevitably would have been acquired through lawful means had the [] misconduct not occurred." *Kennedy*, 61 F.3d at 497; *see also United States v. Alexander*, 540 F.3d 494, 502 (6th Cir. 2008). While a wholly independent investigation is one way for the government to show inevitable discovery, that is not the only way to make the required showing. *See id.* at 499-500. Instead, the government may show "compelling facts indicating that the disputed evidence inevitably would have been discovered." *Id.* at

[12] Defendants also argue that the real-time cell-site location data led to the traffic stops. Because the Court has already found the location data admissible under the good-faith exception, the Court need not consider whether the data led to a search where the evidence collected was "tainted." Therefore, in this section, the Court addresses only the evidence gathered from the use of GPS tracking data on Eric Powell's vehicle.

498; *see also United States v. Akridge*, 346 F.3d 618, 623 (6th Cir. 2003) (quoting *Murray v. United States*, 487 U.S. 533, 539 (1988) ("The inevitable discovery doctrine, with its distinct requirements, is in reality an extrapolation from the independent source doctrine: Since the tainted evidence would be admissible if in fact discovered through an independent source, it should be admissible if it inevitably would have been discovered."). The government must show inevitable discovery by a preponderance of the evidence. *Id.* at 497.

Finally, the attenuation doctrine states that if evidence seized is sufficiently "attenuated" from the initial Fourth Amendment wrongdoing, the taint may also be so attenuated as to permit the admission of the evidence. *United States v. Williams*, 615 F.3d 657, 668-69 (6th Cir. 2010). A court must consider "[t]he temporal proximity of the [(unlawful search)] and the [emergence of the incriminating evidence at issue], the presence of intervening circumstances, and, particularly, the purpose and flagrancy of the official misconduct." *Id.* (brackets in original) (citing *Brown v. Illinois*, 422 U.S. 590, 603-04 (1975)). "No single factor in this analysis is dispositive of attenuation." *United States v. Beauchamp*, 659 F.3d 560, 573 (6th Cir. 2011).

2. Analysis

The Court will apply the above standards to the traffic stops, in chronological order.

a. Whigham Traffic Stop

The first challenged stop after the GPS tracker was placed on Eric Powell's truck, was the traffic stop of Benny Whigham's vehicle on June 23, 2010. On June 22, 2010, the DEA determined, using the GPS tracker, that Eric Powell had traveled from Detroit to Chicago. At some point while Powell was in Chicago, the DEA lost the GPS tracker signal from

Powell's truck, and deployed agents to locate the truck visually. Hr'g I at 38-40. The next day, the DEA began physical surveillance of Powell's truck and Whigham's vehicle, following the vehicles to Cicero, Illinois. *Id.* In Cicero, Powell, Whigham, and Earnest Proge left the two vehicles in a restaurant parking lot for a period of time during which an unknown Hispanic male took Whigham's vehicle to a garage, and then returned it to the parking spot several minutes later. *Id.* at 40. The agents, assisted by the Michigan State Police, continued physical surveillance of the vehicles for over ten hours, as they were driven in tandem from Cicero back toward Detroit. Sullivan Aff. ¶ 11, ECF No. 74-9. A state trooper stopped Whigham's vehicle for a traffic violation near Ann Arbor, Michigan. Hr'g I at 44. Whigham granted the police consent to search the vehicle. *Id.*; Sullivan Aff. at ¶ 13. The trooper found thirteen kilograms of heroin in the vehicle. *Id*.

The traffic stop and search are sufficiently attenuated from use of the GPS tracker to preclude application of the exclusionary rule. As stated above, the factors relevant to attenuation are (1) the length of time between the illegal search and discovery of new evidence; (2) the presence of intervening circumstances; and (3) the purpose and flagrancy of the official misconduct. *United States v. Gross*, 662 F.3d 393, 401-402 (6th Cir. 2011).

Here, the time factor is neutral; the GPS tracker was used to locate Eric Powell's vehicle in Chicago nearly a full day before the traffic stop of Whigham's vehicle. Even if the gap between use of the GPS tracker and the traffic stop can be considered close in time, temporal proximity alone, does not justify suppression. *See generally Clariot*, 655 F.3d at 555 ("[N]o case (to our knowledge) holds that temporal proximity alone, without any other indicia of causation, justifies suppression.").

Next, multiple intervening circumstances occurred between the use of the GPS tracker and the vehicle stop that were sufficient to dissipate any unlawful conduct. First, the GPS tracker was not used to track Whigham's vehicle at all. Second, Whigham's vehicle was directly observed by several DEA agents that day, both in the city and on the highways. The DEA would have inevitably discovered Whigham's vehicle on the highway, regardless of any use of the GPS tracking device on Eric Powell's truck that day. Third, Whigham's vehicle was lawfully stopped by the MSP. Although the stop was pretextual, nothing in the record shows that Whigham did not actually violate the traffic laws justifying the stop. *See United States v. Herbin*, 343 F.3d 807, 809 (6th Cir. 2003) (even if pretextual, a traffic stop for an actual violation of the traffic laws remains legal). Finally, during the traffic stop, Whigham gave the MSP his consent to search the car. *See United States v. Burton*, 334 F.3d 514, 519 (6th Cir. 2003) (officers may reasonably request consent to search during a traffic stop even absent other evidence). While the exclusionary rule may in certain circumstances still exclude evidence when a consent to search was given, consent that is "sufficiently attenuated" from the original seizure remains valid. *See United States v. Lopez-Arias*, 344 F.3d 623, 629 (6th Cir. 2003). Here, for the circumstances discussed above, Whigham's consent was sufficiently attenuated from initial use of the GPS tracker to locate Powell's truck in Chicago to remain admissible.

Finally, the agents' conduct was not flagrant. Donovan had no reason to believe installation of the tracker was illegal. To the contrary, he consulted extensively with the U.S. Attorney's Office and the DEA general counsel's office regarding use of the tracker, and he testified that he would have, and could have, obtained a warrant had he felt it necessary. *See* Hr'g II; *see also United States v. Boone*, 62 F.3d 323, 325 (10th Cir. 1995)

(finding that the officer's mistaken belief that defendants had consented to search, while a Fourth Amendment violation, "does not qualify as flagrant misconduct that would tilt the scales against attenuation"). Accordingly, the Court finds that the evidence seized during the traffic stop of Whigham's car is admissible.

b. Valle Traffic Stop

On June 28, 2010, the DEA was conducting surveillance of a suspected stash location, a residence at 20109 Conley Street, Detroit, Michigan, using pole cameras and physical surveillance. Nov. 8 Donovan Aff. ¶ 61, ECF No. 74-13; Resp. at 37-38. The DEA observed Juan Valle arrive at the residence, followed shortly thereafter by Carlos Powell. Powell carried a large bag with him into the residence. When Valle emerged later, he placed several objects into his vehicle and drove away. Nov. 8 Donovan Aff. ¶ 61-62. The DEA coordinated with the Michigan State Police in Charlotte, Michigan, to track Valle's vehicle. State troopers stopped the vehicle after a traffic violation. Valle gave them his consent to search the vehicle. Resp. at 38. State troopers found roughly $259,000 in the vehicle. *Id.* at ¶ 63.

Although the GPS tracking device was attached to Eric Powell's vehicle during this period, nothing in the record demonstrates that the tracking information had anything to do with the stop of Valle's vehicle. Donovan testified specifically that GPS location data from Eric Powell's vehicle was not used in the events surrounding this search. Hr'g I at 48. Accordingly, the Court finds the GPS tracking data played no, or a highly attenuated, role in this search. Because the traffic stop was legal and Valle consented to search, all evidence from the search is admissible.

c. Proge Traffic Stop

Over the course of several weeks of investigation, which included some use of the GPS tracker, the DEA determined that on several occasions Eric Powell and Earnest Proge drove in tandem between Detroit and Michigan. Nov. 8, 2010 Donovan Aff. ¶ 68. On September 17, 2010, while the GPS tracker was still attached to Powell's truck, the DEA used surveillance cameras to independently observe Powell arrive at a residence in Eastpointe, Michigan, and, wearing latex gloves, load several large suitcases into Proge's Ford Flex. Hr'g I at 51; Nov. 8, 2010 Donovan Aff. ¶ 69. Powell drove the Ford Flex to a warehouse in Centerline, Michigan where the DEA continued surveillance of the vehicle using a different pole camera. *Id.* Later, the Ford Flex, now driven by Proge, departed from the warehouse. From their knowledge of Powell and Proge's previously tracked trips, the DEA dispatched agents along Interstate 94 to look for the Ford Flex. Hr'g I at 53. An agent spotted the vehicle proceeding west on Interstate 94 toward Kalamazoo, traveling in tandem with Powell's truck. *Id.* at 53; Nov. 8, 2010 Donovan Aff. ¶ 70. The GPS device may or may not have been used to locate Powell's truck at the same time, but Donovan testified that in his opinion, the DEA would inevitably have located Proge's vehicle on the highway at some point that day because of the multiple DEA and Michigan State Police officers searching the highway for the vehicle. *Id.* at 57.

State troopers stopped Proge's vehicle in Calhoun County, after a traffic violation. Nov. 8 Donovan Aff. ¶ 71. Proge at first complied with the stop, but then fled the scene, nearly striking another police officer who had just arrived. Hrg. I at 59. Proge engaged the Michigan State Police in a high-speed chase before pulling over. The police arrested Proge for felony Fleeing and Eluding and Assault of a Police Officer, and searched his car. During the search of the vehicle, troopers discovered more than $2.2 million, as well as a drug

ledger, and a newspaper article regarding a Detroit Police Department drug raid. *Id.*; Nov. 8 Donovan Aff. at ¶¶ 71-73.

"If a suspect's response to an illegal stop is a new and distinct crime, such as flight or use of force, any evidence recovered incident to the arrest for the subsequent crime is not tainted by the unlawfulness of the initial detention." *Beauchamp*, 659 F.3d at 574. The search of Proge's vehicle occurred only after his arrest for unlawful flight, thereby serving to attenuate whatever illegal taint the GPS tracker may have initially provided. *See Baldwin*, 114 F. App'x at 682 (finding evidence inadmissible where it was discovered *before* defendant's illegal conduct). The Court will therefore admit all evidence from this stop.

d. de Vallejo Traffic Stop

The final challenged traffic stop is the search of Margarita de Vallejo's car on October 22, 2010. Donovan had removed the GPS tracker from Eric Powell's truck sometime on September 17, 2010, because he believed its use may have caused suspicion among the drug traffickers. Hr'g I at 60. But on October 1, 2010, after learning that Eric Powell had apparently taken another trip to Chicago for the purpose of exchanging drugs, Donovan replaced the tracker. *Id*. at 61.

On October 22, 2010, the DEA, using a pole camera, observed Powell loading several suitcases from the Eastpointe residence onto his truck. Nov. 8 Donovan Aff. ¶ 89, ECF No. 74-14. The DEA again established surveillance along I-94 to look for the truck, as well as for a Ford Taurus that agents knew Proge had taken to driving. Hr'g I at 63. Agents spotted the vehicles on I-94 near Romulus, and followed them to the parking lot of a hotel in Ann Arbor. *Id.* at 63-65. Donovan testified that, although agents used the GPS tracking device to help track Powell's movements, the DEA had a sufficient police presence on the road

that the agents would inevitably have been able to physically track Powell's truck for the duration of the day. *Id.* at 64. At the hotel, the DEA observed Powell and Proge transfer the suitcases from the truck into a Toyota Camry parked behind the hotel. *Id.* at 65; Nov. 8 Donovan Aff. ¶ 94. The DEA agents followed the Toyota, driven by de Vallejo, away from the encounter, and did not follow Powell's truck. The agents then, in conjunction with the Michigan State Police, stopped the Toyota after de Vallejo committed a traffic violation. *Id.* During the stop, de Vallejo gave the officers her consent to search the vehicle. Nov. 8 Donovan Aff. ¶ 95. Officers found 12 kilograms of cocaine and roughly $2 million in currency in the car. *Id.* at ¶ 96.

Based on the facts presented, the Court finds the inevitable-discovery and attenuation doctrines permit admission of the evidence found in de Vallejo's vehicle. First, although it is true that agents used the GPS tracker during the pursuit of Eric Powell's vehicle, they did so only after they had observed via the pole camera behavior indicating he was preparing to engage in another illegal drug or money transfer trip. Moreover, as Donovan testified, agents and state troopers were dispatched to locate the truck on the interstate and would inevitably have done so and been able to physically track Powell and Proge as they traveled to Ann Arbor where they met de Vallejo. For these reasons, the Court finds that the agents would inevitably have discovered de Vallejo's involvement, even without the GPS tracking evidence.

Second, like the Whigham stop, the police detained de Vallejo pursuant to a lawful traffic stop, and de Vallejo gave her consent to search. Based on these intervening circumstances, and applying the same legal standards discussed during the Whigham analysis, the Court finds that the agent's use of the GPS device to track Powell was so

attenuated from the DEA's actions in stopping de Vallejo's vehicle that the evidence seized in the stop is admissible.

IV. Warrants Issued for the Search of Nine Detroit Properties

Finally, Defendants challenge the warrants issued on November 8, 2010, for the searches of nine properties in the Detroit metro area. Defendants do not challenge the searches directly, but rather challenge them under the fruit-of-the-poisonous-tree doctrine, arguing that the warrants were premised on information obtained through the contested searches discussed above. The nine properties are:

- 20109 Conley Street, Detroit, Michigan; a stash house / safe house used by Carlos Powell and his organization.
- 15765 Stricker, Eastpointe, Michigan; a stash house / safe house used by Carlos and Eric Powell to facilitate their operation.
- 15514 E. Eight Mile Road, Detroit, Michigan; a commercial store front owned and operated by Carlos Powell.
- 22208 Raven Avenue, Eastpointe, Michigan; a residence used by Carlos Powell and Tamika Turner.
- 57869 Apple Creek Drive, Washington Township, Michigan; a residence used by Carlos Powell and Tamika Turner.
- 6748 Oyster Cove, West Bloomfield, Michigan; a residence owned by Carlos Powell.
- 24505 Franklin Farms Drive, Franklin, Michigan; a residence used by Eric Powell.
- 24300 Sherwood Avenue, Centerline, Michigan; a commercial warehouse operated and utilized by Eric Powell.
- 1137 Outer Drive, Detroit, Michigan; a residence used by Earnest Proge.

In applying for the relevant warrants, Donovan prepared a seventy-six page affidavit. *See* Nov. 8 Donovan Aff. In the affidavit, Donovan first reiterated the identity of Morowa as an informant who identified Carlos Powell as a major drug trafficker; and then he proceeded

to outline the course of the investigation until that point, including the seizure of $1.1 million in Phoenix, Arizona, in April 2010; the interview of another incarcerated participant in the trafficking ring; the seizure of 13 kilograms of heroin in June; the seizure of $5 million in Chicago in July; surveillance of Carlos Powell and Eric Powell via pole cameras and GPS tracking devices; the seizure of $2 million and 12 kilograms of cocaine in October; and the results of financial and income tax investigations and analysis. *Id.* at ¶¶ 8-53.

The crux of Defendants' argument is that evidence derived from the cell-site and GPS location data from the phones, and from the GPS tracking device on Powell's truck, formed so substantial a part of the November 8 Donovan Affidavit as to taint the warrants with illegality under the fruit-of-the-poisonous-tree doctrine, thereby requiring suppression of the evidence seized from the properties. The Court finds that all the evidence is admissible.

First, the Court has already admitted the cell-site and GPS location data from the cell phones under the good-faith exception. To the extent, therefore, the warrants are premised on information obtained from the cell-phone tracking, the evidence is untainted. *See United States v. Jenkins*, 396 F.3d 751, 760 (6th Cir. 2005) (court may consider untainted portions of warrant affidavit to determine whether probable cause exists). The same is true of the evidence obtained from the vehicle searches. And when considering that evidence along with the rest of the affidavit as the basis for probable cause, the affidavit clearly establishes probable cause to search. Even if the Court did not consider the GPS tracking data, there would remain an overwhelming amount of evidence documented in the affidavit including the vehicle searches, phone records, witness affidavits, and other evidence that is more than sufficient to constitute a substantial basis for the Magistrate Judge to conclude that probable cause existed to search the nine properties. *See Gardiner*, 463 F.3d at 470

(magistrate need only a substantial basis to support a finding of probable cause). The warrants remain valid.

And even considering the warrant absent the GPS data (which, as stated, would not exclude the previously admitted vehicle searches), any evidence seized from the properties would nevertheless remain admissible under the valid-warrant good faith exception. *See Buford*, 632 F.3d at 271. The DEA was relying on a warrant issued by a magistrate judge, and none of the four Leon exceptions exclude the evidence. *See Leon*, 468 U.S. at 914 (limits to good faith exception). No argument is made, nor does any evidence reveal, that the affidavit contained any factually false information; or that the Magistrate Judge abandoned the neutral and detached role. And the affidavit, having a substantial basis, clearly was not lacking in indicia; nor is there any suggestion the affidavit on its face was deficient. The Court will admit all the evidence seized from the properties.

CONCLUSION

As set forth above, with respect to the real-time cell-site location data, the Court finds that the government did not adequately establish probable cause for the warrants to issue, but the evidence obtained from the cell-phone tracking is admissible under the good-faith exception. With respect to the installation and use of the GPS tracking device, whether or not a reasonable search, the inevitable-discovery, independent-source, or attenuation exceptions permit the admission of all the tracking data gathered, as well as the evidence obtained in the search of Whigham's, Proge's, and de Vallejo's vehicles. The evidence obtained in the search of Valle's vehicle is also admissible. Finally, the evidence obtained

in the searches of the nine Detroit properties is admissible under the good-faith exception. For these reasons, and those stated in the Court's prior order addressing the motion, Defendants' motion to suppress is denied in full.

ORDER

WHEREFORE, it is hereby **ORDERED** that the Motion to Suppress (docket no. 74) is **DENIED**.

SO ORDERED.

s/Stephen J. Murphy, III
STEPHEN J. MURPHY, III
United States District Judge

Dated: May 3, 2013

I hereby certify that a copy of the foregoing document was served upon the parties and/or counsel of record on May 3, 2013, by electronic and/or ordinary mail.

Carol Cohron
Case Manager