UNITED STATES DISTRICT COURT EASTERN DISTRICT OF MICHIGAN SOUTHERN DIVISION

UNITED STATES OF AMERICA,

DI	-:	tiff
М	ann	11111

Case Number 13-20423 Honorable David M. Lawson

v.

JIMMIE EUGENE WHITE II,

L	erenc	iant.		

OPINION AND ORDER DENYING MOTION TO SUPPRESS EVIDENCE

Defendant Eugene Jimmie White II, charged with drug distribution crimes, has filed a motion to suppress evidence obtained through the execution of search warrants for active real time cell site and GPS location data monitoring, including a search warrant for his residence based on information he believes was derived from the monitoring data. The government argues that White does not have "standing" to challenge the tracking data for certain cell phones that did not belong to him. Although the standing argument is imprecise, the Court finds that White did not have a reasonable expectation of privacy in those phones. The government also argues that the search warrants issued to track White's cell phone were supported by probable cause sufficient to authorize tracking for an open-ended time period and into private spaces. The Court cannot agree with that argument. However, the good faith exception to the exclusionary rule saves the evidence. And the search warrant for White's house was based on information independent of the tracking data to establish probable cause. Therefore, the motion to suppress will be denied.

On May 14, 2010, Drug Enforcement Agency ("DEA") agents executed a federal search warrant at Jimmie White's home in Detroit. They recovered cash, 898 pills of N-Benzylpiperazine Dihydrochloride (BZP), a Cobray 9 mm pistol with an obliterated serial number, and magazines loaded with various types of ammunition. The execution of the search warrant was the culmination of a months-long investigation into ecstasy trafficking in Detroit. The investigation into White's drug trafficking activity included a variety of investigative techniques, including a Title III wiretap interception of his cellular phone conversations, state search warrants for cell site and GPS location monitoring of his cellular phone, controlled purchases of ecstasy and BZP by a confidential informant, and surveillance of White's home. The government obtained long-term state search warrants, which are the subject of White's motion, to track the location of White's cellular phone on May 28, 2009, February 5, 2010, and April 29, 2010. The government also obtained state search warrants to track the location of the phones of other people.

White was arrested on May 14, 2010 during the execution of the search warrant at his home, but the arrest was based on an outstanding warrant from Ohio for fraudulent activity. White was not charged with the current offenses until he completed his sentence for the Ohio crimes; the government filed a criminal complaint against White based on its drug conspiracy investigation on April 29, 2013. On June 4, 2013, White was indicated for conspiracy to distribute ecstasy and BZP, possession with intent to distribute BZP, possession of a firearm in furtherance of a drug trafficking offense, and possession of a firearm by a convicted felon.

White filed a motion to suppress evidence on September 4, 2014. The government responded, and the Court heard argument from the parties, including White and his standby counsel,

on September 30, 2014. Because the parties did not address all of the relevant issues, the Court permitted them to file supplemental briefs, which have now been received. The suppression motion is ready for decision.

II.

White asks the Court to suppress evidence obtained from tracking his cell phone, plus tracking data and derivative evidence obtained from cell phones of which he was neither a subscriber nor user. The latter evidence came from search warrants dated February 23, 2010 and February 19, 2010. The government argues that White lacks "standing" to challenge those search warrants.

The "rights assured by the Fourth Amendment are personal rights, and . . . may be enforced by exclusion of evidence only at the instance of one whose own protection was infringed by the search and seizure." *Simmons v. United States*, 390 U.S. 377, 389 (1968) (quoted in *Rakas v. Illinois*, 439 U.S. 128, 138 (1978)). Consequently, White must carry the burden of establishing that his own Fourth Amendment rights were violated. *Rakas*, 439 U.S. at 132 n.1. To do so, he must show (1) that he had a subjective expectation of privacy in the thing that was searched or the items that were seized, and (2) that society is prepared to recognize that expectation as legitimate. *California v. Ciraolo*, 476 U.S. 207, 211 (1986); *United States v. King*, 227 F.3d 732, 743-44 (6th Cir. 2000); *see also United States v. Delgado*, 121 F. Supp. 2d 631, 636 (E.D. Mich. 2000). "Legitimation of expectations of privacy by law must have a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society." *Rakas*, 439 U.S. at 143 n.12.

Characterizing this question as one of "standing," however, miscasts the issue. The Supreme Court rejected the concept of "standing" in *Rakas*, 439 U.S. at 139-40. It is commonly

acknowledged that "in determining whether a defendant is able to show the violation of his . . . Fourth Amendment rights, the 'definition of those rights is more properly placed within the purview of substantive Fourth Amendment law than within that of standing." *Minnesota v. Carter*, 525 U.S. 83, 88 (1998) (quoting *Rakas*, 439 U.S. at 140). More than thirteen years ago, the Sixth Circuit recognized that "the concept of 'standing' has not had a place in Fourth Amendment jurisprudence for more than a decade" and that "the matter of standing in the context of searches and seizures actually involve[s] substantive Fourth Amendment law [in which] . . . a defendant [must] prove a legitimate expectation of privacy as a prerequisite to challenging assertedly unlawful police conduct." *United States v. Smith*, 263 F.3d 571, 581-82 (6th Cir. 2001) (quoting *United States v. Sanchez*, 943 F.2d 110, 113 n.1 (1st Cir. 1991)).

White has not demonstrated a reasonable expectation of privacy in the phones that did not belong to him. "In order to qualify as a person aggrieved by an unlawful search and seizure one must have been a victim of a search or seizure, one against whom the search was directed, as distinguished from one who claims prejudice only through the use of evidence gathered as a consequence of a search or seizure directed at someone else." Rakas, 439 U.S. at 134-35 (internal quotation marks omitted). White may not challenge the seizure of data from someone else's cell phone. See United States v. Forest, 355 F.3d 942, 948 (6th Cir. 2004) (holding that the defendant did not have an expectation of privacy that would allow a challenge to the search of his codefendant's phone), vacated on other grounds, 543 U.S. 1100 (2004). The motion to suppress evidence derived from the February 23, 2010 and February 19, 2010 search warrants, therefore, will be denied.

The investigators obtained warrants on May 28, 2009 and February 5, 2010 from a state magistrate to

search the following described place: Any and all records relating to the location of cellular phone tower(s) including specific active GPS precision tracking of cellular phone number (313) 674-6225. Said records shall include the time period [covering a thirty-day span] on a continuous basis.

(A search warrant also was obtained on April 10, 2010 for cell site and GPS data, but White did not address that warrant in his motion. However, the discussion would be the same if he did.) The affidavit presented in support of the May 28, 2009 warrant request was signed by a DEA agent. He alleged that the DEA had been investigating a drug trafficking organization operating in Detroit that distributed MDMA and marijuana; a confidential source (who was credible) identified defendant Jimmy White II as the leader; White told the source that White obtained MDMA from Canada and marijuana from Arizona and Alabama; and White used the target cell phone to discuss drug distribution. The affidavit also stated that the source contacted White on the target phone to set up controlled purchases, the most recent of which occurred within the previous week. The agent also averred that the target phone was registered to White at an address on Baldwin Street in Detroit, but White's vehicle registration and driver's license listed his address in Romulus, Michigan, causing the agent to conclude that White was "utilizing multiple addresses to disguise his true whereabouts." The agent also averred that White solicited the confidential source's cooperation to locate suppliers outside Michigan, and he told the source that he sold drugs outside Michigan. Finally, to justify the request for continuous, real-time tracking, the DEA agent stated:

[I]n order to determine where the cellular phone is being used, it is necessary that the above stated records be furnished to your Affiant on a continuous basis until the

account is closed, or until known are WHITE II's drug trafficking activities, his residence, his vehicles and his narcotics distribution associates.

The affidavit supporting the February 5, 2010 search warrant was submitted by a Dearborn Heights, Michigan police officer. It was largely the same as the earlier affidavit, except that it noted that the Romulus address was White's mother's house; and it stated that when it tracked White under the previous search warrant, the police officer learned that White made a trip to West Virginia and back in a 24-hour period, leaving and returning in the nighttime hours.

On May 13, 2010, the DEA agent obtained a federal search warrant to search White's house in Detroit. The supporting affidavit recited a brief history of the investigation, including the substance of conversations over White's cell phone intercepted with the authority of a federal wiretap order. The conversations related to the sale and purchase of MDMA pills to a source in Illinois in February 2010. The transaction took place at White's house and was confirmed by surveillance. The affidavit mentioned the previous GPS tracking warrants and that the agent learned that White was receiving phone calls from Illinois.

A.

White argues that the evidence obtained from the GPS tracking data must be suppressed because the search warrant affidavits fail to establish probable cause for long-term, real-time active tracking of White through his cell phone. The government argues that in *United States v. Skinner*, 690 F.3d 772 (6th Cir. 2012), the Sixth Circuit held that a person does not have a reasonable expectation of privacy in the data emanating from his cell phone that showed his location. The government argues that even if acquisition of the tracking data constituted a search, probable cause supported the search warrant authorizing the interception.

Two recent cases bear on the question presented: Skinner and United States v. Jones, 132 S. Ct. 945 (2012), although neither answers the question directly. In *Jones*, the Supreme Court held that attachment of a GPS tracking device to a vehicle without the owner's permission for the purpose of monitoring the vehicle's movements on public streets was a search within the meaning of the Fourth Amendment. Id. at 949. The Court based its holding on the idea that the attachment of the device to the underside of the vehicle, although a minor intrusion, amounted to a physical trespass. And such a "physical[] occup[ation of] private property for the purpose of obtaining information . . . would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted." Ibid. The Court brushed aside the government's argument that the defendant had no reasonable expectation of privacy in the underside of his car or his movement on public roads. Although the Court acknowledged that an intrusion can amount to a search if it trenches upon a person's reasonable expectation of privacy, a formulation of Fourth Amendment jurisprudence that became ascendant in Katz v. United States, 389 U.S. 347, 351 (1967), that "formulation" did not displace the trespassory foundation on which the early Fourth Amendment cases were based. *Id.* at 952 (stating that "the Katz reasonable-expectation-of-privacy test has been added to, not substituted for, the common-law trespassory test").

White's case is similar to *Jones* in that the government engaged in real-time tracking of White's movements over an extended period of time. But it differs from *Jones* in one critical respect: there was no physical intrusion by the government into any of White's real or personal property. The government obtained tracking data from White's cell phone without any physical interference with his property. Therefore, White's case is not controlled by the *Jones* majority opinion.

In Skinner, the Sixth Circuit held in a split decision that the defendant "did not have a reasonable expectation of privacy in the GPS data and location of his cell phone" while traveling on public thoroughfares. 690 F.3d at 777, 781. In that case, law enforcement officers tracked Skinner's phone for three days during his travel on public roads while he transported more than 1,000 kilograms of marijuana between Arizona and Tennessee. The court reasoned that the tracking data was a proxy for physical surveillance, but it also seemed to base its holding on the notion that when a criminal uses a device — here, a pay-as-you-go cell phone — to advance an illegal endeavor, he cannot complain if the device yields information that leads to his detection. See id. at 777-78. Although no authority was cited for the second point, on the first point, the court drew support from United States v. Knotts, 460 U.S. 276 (1983), a case in which the Supreme Court held that no search occurred when federal agents placed a "beeper" tracking device in a drum of chemicals before it was delivered to the defendant, and then tracked the drum's location through a combination of physical surveillance and the signals the beeper emitted. The court of appeals was persuaded by the argument that "'[t]he governmental surveillance conducted by means of the beeper in this case amounted principally to the following of an automobile on public streets and highways.... A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another." Skinner, 690 F.3d at 778 (quoting Knotts, 460 U.S. at 281). As with Skinner's cell phone tracking data, "there [was] no indication that the beeper was used in any way to reveal information . . . that would not have been visible to the naked eye." *Ibid.* (quoting *Knotts*, 460 U.S. at 285). See also United States v. Forest, 355 F.3d 942, 951 (6th Cir. 2004), vacated on other grounds, Garner v. United States, 543 U.S. 1100 (2005) (holding that "pinging" the

defendant's cell phone to gather cell site location data did not violate the Fourth Amendment because agents could have obtained the same information by following the defendant's car).

White's case is similar to *Skinner* in that here the agents used White's cell phone tracking data to follow his movements on public roads. But it differs in another critical respect: the surveillance in this case took place over an extended time period — continuously for 30 days on two (or three) separate occasions — and followed White into both public and private spaces. Justice Alito's concurring opinion in *Jones*, which drew support from a fifth justice, see *Jones*, 132 S. Ct. at 954-57 (Sotomayor, J., concurring), suggested that "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy." Id. at 964 (Alito, J., concurring). The 4-week tracking in that case was well over the line of reasonableness, in his view. *Ibid.* ("We need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark."). And the Skinner majority acknowledged Justice Alito's concerns, allowing that "[t]here may be situations where police, using otherwise legal methods, so comprehensively track a person's activities that the very comprehensiveness of the tracking is unreasonable for Fourth Amendment purposes." Skinner, 690 F.3d at 780. Skinner does not control the present case, because the length and breadth of the tracking here extends well beyond what any reasonable person might anticipate.

In the absence of a trespass, the test that applies is derived from the cases following *Katz*: the defendant must have a "reasonable expectation of privacy" in the thing searched or seized. *Rakas v. Illinois*, 439 U.S. 128, 134 (1978). As suggested by the phrase "reasonable expectation," and as noted above, the defendant both must have a subjective expectation of privacy in the thing or location, and his interest must be one that society recognizes as legitimate, either due to

traditional concepts of property law "or to understandings that are recognized and permitted by society." *United States v. Smith*, 263 F.3d 571, 582 (6th Cir. 2001) (quoting *Rakas*, 439 U.S. at 143 n.12).

In a similar case, my distinguished colleague in this district held that long-term surveillance by means of cellular tracking data constituted a search that must be justified by probable cause and a warrant. United States v. Powell, 943 F. Supp. 2d 759, 770 (E.D. Mich. 2013) (Stephen J. Murphy, J.). Other courts have concurred. See United States v. Davis, 754 F.3d 1205, 1217 (11th Cir. 2014) ("[C]ell site location information is within the subscriber's reasonable expectation of privacy. The obtaining of that information without a warrant is a Fourth Amendment violation."), vacated and rehearing en banc granted, --- F. App'x ---, 2014 WL 4358411 (11th Cir. Sept. 4, 2014); Com. v. Augustine, 467 Mass. 230 (2014) (recognizing a reasonable expectation of privacy in cellular site location information); State v. Earls, 214 N.J. 564, 587-88, 70 A.3d 630, 643 (2013) (finding, under New Jersey's state constitution, that individuals have a reasonable expectation of privacy in the location of their cell phones); In re Application of United States for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 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); United States v. Benford, No. 2:09 CR 86, 2010 WL 1266507, at *2 (N.D. Ind. Marc. 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."); United States 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 location information and finding a Fourth Amendment privacy interest in location); In re the Application of the United States for an Order Authorizing (1) Installation and Use of a Pen Register and Trap and Trace Device or Process, (2) Access to Customer Records, and (3) Cell Phone Tracking, 441 F. Supp. 2d 816, 837 (S.D. Tex. 2006) ("[D]etailed location information, such as triangulation and GPS data, [] unquestionably implicate Fourth Amendment privacy rights."); In re Application the of the United States for an Order Authorizing Installation and Use of a Pen Register and a Caller Identification System on Telephone Numbers (Sealed), 402 F. Supp. 2d 597, 604-05 (D. Md. 2005) (recognizing that monitoring of cell phone location information is likely to violate a reasonable expectation of privacy); In re the Application of the United States for an Order (1) Authorizing the Use of a Pen Register and a Trap and Trace Device, 396 F. Supp. 2d 294, 323 (E.D.N.Y. 2005) ("Because the government cannot demonstrate that cell site tracking could never under any circumstance implicate Fourth Amendment privacy rights, there is no reason to treat cell phone tracking differently from other forms of tracking ... which routinely require probable cause.").

It is not difficult to reach the same conclusion here. White certainly had a subjective expectation in his movements over time. In fact, the second search warrant affidavit made the point of noting that White's trip to West Virginia took place at night, and that criminals frequently travel during those hours to conceal their movements. And there are several reasons to conclude that

society would recognize that privacy interest as legitimate. For one, White's movement into private spaces, including the interior of his own house, touches on privacy interests that lie "[a]t the very core' of the Fourth Amendment." *Kyllo v. United States*, 533 U.S. 27, 31 (2001) (quoting *Silverman v. United States*, 365 U.S. 505, 511 (1961)); *see also United States v. Karo*, 468 U.S. 705, 717 (1984) (rejecting the idea that the government "should be able to monitor beepers in private residences without a warrant if there is the requisite justification in the facts for believing that a crime is being or will be committed and that monitoring the beeper wherever it goes is likely to produce evidence of criminal activity"). In *Kyllo*, the Court endorsed the general principle that the use of technology to collect information that otherwise could not have been obtained without a physical intrusion amounts to a search.

Moreover, Congress has obligated cell phone service providers to protect the proprietary information of its customers, including location data. 47 U.S.C. § 222(a) (stating that "[e]very telecommunications carrier has a duty to protect the confidentiality of proprietary information of [its]... customers"). Using a cell phone does not amount to consenting to the dissemination of "call location information." 47 U.S.C. § 222(f)(1) (stating that "without the express prior authorization of the customer, a customer shall not be considered to have approved the use or disclosure of or access to . . . call location information concerning the user of a commercial mobile service" except in cases of defined emergencies). Customers reasonably may expect their providers to comply with the law.

One more reason for recognizing White's expectation as objectively reasonable was expressed by Justice Sotomayor in *Jones*:

In cases involving even short-term monitoring, some unique attributes of GPS surveillance relevant to the *Katz* analysis will require particular attention. GPS

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) (citing *People v. Weaver*, 12 N.Y.3d 433, 441-42, 882 N.Y.S.2d 357, 909 N.E.2d 1195, 1199 (2009) ("Disclosed in [GPS] data . . . will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on")). It is safe to say that society would recognize that an interest in keeping these movements private is "reasonable."

There is a problem, of course, in deciding when the aggregation of data showing movement in public spaces crosses the line and becomes a "search." *See*, *e.g.*, Orin Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 Mich. L. Rev. 311, 330-36 (2012). However, courts have confronted similar problems in the past. For instance, how long may law enforcement detain property waiting for a drug detection dog to arrive for a sniff before the intrusion matures into a "seizure"? To find an answer, courts must "balance the nature and quality of the intrusion on the individual's Fourth Amendment interests against the importance of the governmental interests alleged to justify the intrusion." *United States v. Place*, 462 U.S. 696, 703 (1983).

Under that rationale, it may be appropriate to track an individual for a short time on public streets based on a level of suspicion that is less than probable cause. *See Terry v. Ohio*, 392 U.S. 1, 22 (1968) (recognizing that society's "general interest [in] . . . effective crime prevention and detection . . . [requires] that a police officer may in appropriate circumstances and in an appropriate manner approach a person for purposes of investigating possibly criminal behavior even though

there is no probable cause to make an arrest"); *cf. Michigan v. Summers*, 452 U.S. 692, 702-703 (1981) (justifying detention of occupants of a home during the execution of a search warrant by the state's interest in "preventing flight in the event that incriminating evidence is found," "minimizing the risk of harm to the officers," and facilitating "the orderly completion of the search"). Longer surveillances may require more justification, and a case might be made that the government's reasons underlying the need for tracking — in the case of domestic terrorism, for example — may call for less. The present case involves a garden-variety drug trafficking crime, nothing more. The blanket surveillance of an individual for thirty days at a time cannot equate to a brief detention, however. The "nature and quality" of an intrusion of that magnitude (in excess of the "the 4-week mark") tips the balance in favor of the individual; it constitutes a breach of one's reasonable expectation of privacy that requires the state to demonstrate probable cause as a justification for the intrusion. *Jones*, 132 S. Ct. at 964 (Alito, J., concurring).

B.

Congress has authorized judicial officers to issue search warrants for "tracking devices." 18 U.S.C. § 3117(a). There is disagreement among the courts on whether a cell phone fits within the statutory definition of a "tracking device": "As used in this section, the term 'tracking device' means an electronic or mechanical device which permits the tracking of the movement of a person or object." 18 U.S.C. § 3117(b). A plain reading suggests that a cell phone emitting geolocation data fits the bill. *See, e.g., In re Order Authorizing Prospective and Continuous Release of Cell Site Location*, --- F. Supp. 2d ----, 2014 WL 3513120, at *5-7 (S.D. Tex. 2014 July 15, 2014). Courts holding otherwise focus on language in the statute that refers to "installation" of such devices, reasoning that cell phones are not government property that are installed in or onto the property of

a user; and also reference a discussion of examples of tracking devices in the legislative history, which focuses on 1986-era "beepers." *See, e.g., In re Smartphone Geolocation Data Application*, 977 F. Supp. 2d 129, 149-50 (E.D.N.Y. 2013).

The former line of cases is better reasoned. Although 18 U.S.C. § 3117(a) refers to "installation" ("If a court is empowered to issue a warrant or other order for the installation of a mobile tracking device, such order may authorize the use of that device within the jurisdiction of the court, and outside that jurisdiction if the device is installed in that jurisdiction." (emphasis added)), the language of the statute does not imply that a device must be "installed" to constitute a tracking device. Subsection (a) addresses the territorial authority of a court issuing the warrant, not the elements of a "tracking device" (which is left to subsection (b)) Moreover, the Congressional Record discussion of beepers is not a definition that ever "made it into the statute." In re Application for Pen Register and Trap/Trace Device with Cell Site Location, 396 F. Supp. 2d 747, 753-54 (S.D. Tex. 2005) (citing S. Rep. No. 541, 99th Cong., 2d Sess., at 10 (1986), reprinted at 1986 U.S.C.C.A.N. 3555, 3564). And a truer reading of the legislative discussion suggests that "its description of technology was merely 'illustrative, not definitional.'" Cell Site, 2014 WL 3513120, at *6 (quoting *United States v. Ramirez*, 112 F.3d 849, 852 (7th Cir. 1997)). Certainly, the main purpose of cell phones is not to function as a law enforcement tracking tool. But they do perform multiple functions; and their technology has caused some to describe them as "the world's most effective tracking devices." *Ibid.* (quoting Julia Angwin, *Dragnet Nation* 141 (2014)).

Moreover, as at least one court has observed, "installation" can denote more than a physical intrusion; it can also contemplate electronic intrusions, such as by "installing" software (either with consent or surreptitiously) with "a screen tap or keystroke." *Ibid.* A cramped reading of the

definition of "tracking device" — one not suggested by the plain language — would not credit Congress for implementing "a uniform and coherent legal regime for tracking devices," *id.* at *7, instead suggesting the imposition of a "a fragmented scheme with varying standards dependent upon the type of technology used," *ibid.*

The same can be said for the tracking device language in Federal Rule of Criminal Procedure 41 (governing search warrants). Certainly the rule aims to regulate the "installation of tracking devices." *E.g.*, Rule 41(b)(4) (authorizing a magistrate judge "to issue a warrant to install within the district a tracking device"); (f)(2) (requiring the executing officer to note "the exact date and time the device was installed"). But Rule 41 also speaks to the *use* of the device as well. *Id.* at (b)(4) (stating that the search warrant "may authorize use of the device to track the movement of a person or property"); (f)(2) (stating that the executing officer must also note "the period during which [the tracking device] was used"). That terminology does not exclude cell phones from the definition of "tracking device"; it functionally includes them. And it reflects the views expressed by the several opinions in *United States v. Jones* that the Fourth Amendment protects against both unreasonable trespassory intrusions (installation) and breaches of privacy rights (use).

Courts that resist the treatment of cell phones as tracking devices express concern that doing so would bring them under the statutory umbrella of the Electronic Communications Privacy Act (ECPA) and Rule 41. *See, e.g., Smartphone*, 977 F. Supp. 2d at 149-50; *Powell*, 943 F. Supp. 2d at 777. That concern is beside the point here. Once it has been determined that acquiring tracking data long-term constitutes a search requiring probable cause, it follows logically that the police must obtain a search warrant. A search conducted without a warrant is "*per se* unreasonable under the Fourth Amendment, — subject only to a few specifically established and well-delineated

exceptions." *Katz*, 389 U.S. at 357 (1967) (footnotes omitted); *see also United States v. Jenkins*, 92 F.3d 430, 436 (6th Cir. 1996). None of those exceptions applies here.

C.

The agents and officers did obtain search warrants that authorized them to gather the tracking data in this case and follow White in real time. The government argues that the supporting affidavits established probable cause for those warrants. White contends that the warrants are overbroad because they authorize the police to track him everywhere and continuously for 30 days at a time.

A search warrant may be issued to seize "any property that constitutes evidence of a criminal offense in violation of the laws of the United States." 18 U.S.C. § 3103a(a); *see also Warden, Md. Penitentiary v. Hayden*, 387 U.S. 294, 306-07 (1967); Fed. R. Crim. Pro. 41(c). "Property' includes . . . information." Fed. R. Crim. Pro. 41(a)(2)(A). When searching for evidence, the police must demonstrate "cause to believe that the evidence sought will aid in a particular apprehension or conviction." *Warden*, 387 U.S. at 307.

But search warrants may not issue except "upon probable cause, . . . and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. The particularity requirement limits the scope of the authorized search, "makes general searches . . . impossible[,] and prevents the seizure of one thing under a warrant describing another." *Marron v. United States*, 275 U.S. 192, 196 (1927). And the scope of the search is tied directly to the finding of probable cause that authorizes it: "The scope of a search is limited to those places in which there is probable cause to believe an item particularly described in the warrant might be found." *Horton v. California*, 496 U.S. 128, 143 n.1 (1990) (Brennan, J., dissenting).

This limiting principle cabins the authority of the police, so that "nothing is left to the discretion of the officer executing the warrant." *Marron*, 275 U.S. at 196. The Fourth Amendment prohibits a magistrate from issuing a "general warrant," *Stanford v. State of Tex.*, 379 U.S. 476, 480 (1965), that is, a license to engage in a "general, exploratory rummaging in a person's belongings," *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971); *see also Ellison v. Balinski*, 625 F.3d 953, 958 (6th Cir. 2010) (explaining that "[t]he history of the Fourth Amendment [demonstrates that it] was enacted in part to curb the abuses of general warrants, devices which provided British officers with broad discretion to search the homes of citizens of the Colonies for evidence of vaguely specified crimes"); *see also Warden*, 387 U.S. at 301 (stating that the Fourth Amendment "was a reaction to the evils of the use of the general warrant in England and the writs of assistance in the Colonies, and was intended to protect against invasions of 'the sanctity of a man's home and the privacies of life,' from searches under indiscriminate, general authority" (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)).

Searches, and the corresponding seizures, "should be as limited as possible." *Coolidge*, 403 U.S. at 467. However, "[t]he degree of specificity required is flexible and will vary depending on the crime involved and the types of items sought." *United States v. Greene*, 250 F.3d 471, 477 (6th Cir. 2001); *see also Guest v. Leis*, 255 F.3d 325, 336 (6th Cir. 2001) ("A search warrant must particularly describe the things to be seized, but the description, whose specificity will vary with the circumstances of the case, will be valid if it is as specific as the circumstances and the nature of the activity under investigation permit.") (internal quotation marks omitted). As the Sixth Circuit explained recently, "[t]he cases on particularity are actually concerned with at least two rather different problems: one is whether the warrant supplies enough information to guide and control the

agent's judgment in selecting what to take; and the other is whether the category as specified is too broad in the sense that it includes items that should not be seized." *United States v. Richards*, 659 F.3d 527, 537 (6th Cir. 2011) (quoting *United States v. Upham*, 168 F.3d 532, 535 (1st Cir.1999)).

The parties have not cited any appellate authority addressing the showing necessary to establish probable cause for a tracking warrant, and the Court has not located any. It has been suggested that the government must show, at a minimum, 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"; and that "the specific cell phone, as well as the person to be tracked, is relevant to the investigation." *Powell*, 943 F. Supp. 2d at 778-79. The government certainly satisfied the second requirement: the affidavit plainly established that White was involved in drug trafficking throughout several states and Canada and used his cell phone to set up and consummate transactions. The first requirement, however, is problematic. If law enforcement anticipates that a suspect will commit a crime *some place* at some future date, does that mean that law enforcement has probable cause to track a suspect *every place* he goes? The answer must be "No," lest general warrants be revived and the Fourth Amendment's particularity requirement be eviscerated.

The government's justification for the broad and far-reaching tracking warrant in this case amounted to an assertion that White was a drug dealer operating in several regions, and therefore the police needed to track him electronically wherever he went. Historically, the limits on such blanket surveillance were practical: "limited police resources and community hostility." *Illinois v. Lidster*, 540 U.S. 419, 426 (2004). But technology has allowed law enforcement to "evade[] the ordinary checks that constrain abusive law enforcement practices." *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring). In the context of tracking-by-cell-phone, the challenge to — indeed,

the obligation of — courts is to articulate "limits . . . upon this power of technology to shrink the realm of guaranteed privacy." *Kyllo*, 533 U.S. at 34. That challenge is met by applying the familiar particularity requirement and "the Fourth Amendment's bedrock principle of reasonableness on a case-by-case basis." *United States v. Richards*, 659 F.3d 527, 538 (6th Cir. 2011).

Once again, a search warrant, including a warrant to track a suspect, must "particularly describ[e] the place to be searched." U.S. Const. amend. IV. Thus, when a law enforcement officer is queried by a magistrate as to where he wants to electronically track a suspect's movements, "everywhere" seldom, if ever, will be an acceptable answer. Cf. Richards, 659 F.3d at 537 (reiterating that "the chief purpose of the particularity requirement [is] to prevent general searches by requiring a neutral judicial officer to cabin the scope of the search to those areas and items for which there exists probable cause that a crime has been committed") (internal citation and quotation marks omitted). In this case, the affidavits did not limit the tracking request to a particular place: they contained no information about any specific place that the government anticipated that White might travel. Instead, the government sought power to electronically track White without limitation every place that he traveled. However, there was no showing that would justify an intrusion of that magnitude; there was no probable cause for a blanket, 30-day search. "The fact that there is probable cause to arrest a person for a crime does not automatically give police probable cause to search his residence or other area in which he has been observed for evidence of that crime. If the rule were otherwise, 'there would be no reason to distinguish search warrants from arrest warrants[.]" United States v. Savoca, 739 F.2d 220, 224-25 (6th Cir. 1984) (quoting United States v. Lucarz, 430 F.2d 1051, 1055 (9th Cir. 1970)).

The police could have satisfied the particularity requirement by presenting a more tailored application for a warrant to track White's movements. For instance, the agent could have explained in his application that he wanted to track White for a limited period based on credible information that White was planning to engage in a drug transaction with the confidential informant at a particular time and place. Or he could have offered information that White was traveling to meet with his Canadian, Arizona, or Alabama suppliers, even if White stayed at motels or the homes of co-conspirators along the way. Or if the agent wanted to track White between his home in Detroit and his mother's home in Romulus, he could have averred that White stored drugs in one location and sold them out of another. That may have required more investigative work (although it appears that the police invested considerable time and resources into this investigation). See Powell, 943 F. Supp. 2d at 780 (noting that "[i]n 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"). The resulting search warrant then could have been limited accordingly. But none of that information was offered to the magistrate, and the police failed to provide any specific reason why they needed to track White for a prolonged duration and in protected areas such as White's home.

The search warrant in this case allowed the police to track White at all times, night and day, on public streets and in private places, and into areas traditionally protected by the Fourth Amendment. *See Karo*, 468 U.S. at 714 (holding that the police may not use a beeper to track a suspect's location in a protected area, such as a residence, without a warrant, because "private residences are places in which the individual normally expects privacy free of governmental

intrusion not authorized by a warrant, and that expectation is plainly one that society is prepared to recognize as justifiable"). The government concedes that it tracked White even when he "was not on public thoroughfares." Gov.'s Resp. at 5. The warrant contained no minimization requirement, *cf.* 18 U.S.C. § 2518(5) (requiring communication intercepts authorized under Title III to "be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under" law), or any other provision that defined "the discretion of the officer executing the warrant," *Marron*, 275 U.S. at 196, or "the limits of his power to search," *Groh v. Ramirez*, 540 U.S. 551, 561 (2004) (quoting *United States v. Chadwick*, 433 U.S. 1, 9 (1977)). The tracking warrants were akin to the general warrants condemned by the Founders, *see Steagald v. United States*, 451 U.S. 204, 220 (1981), and are repugnant to the Fourth Amendment.

IV.

The government argues that even if the tracking searches are unconstitutional, the evidence should not be excluded because the police relied in good faith on the search warrants. Exclusion of illegally obtained evidence, a judicial remedy of "last resort," *Herring v. United States*, 555 U.S. 135, 141 (2009) (quoting *Hudson v. Michigan*, 547 U.S. 586, 591 (2006), is not mandated by the Fourth Amendment; instead it is a court-created rule intended to "compel respect for the constitutional guaranty" found in the Fourth Amendment. *Davis v. United States*, --- U.S. ---, 131 S. Ct. 2419, 2426 (2011) (internal citations and quotation marks omitted).

When a search warrant is not supported by probable cause, the evidence obtained need not be suppressed if it was "seized in reasonable, good-faith reliance on a search warrant that is subsequently held to be defective." *United States v. Hython*, 443 F.3d 480, 484 (6th Cir. 2006) (quoting *United States v. Leon*, 468 U.S. 897, 905 (1984)). "[T]he relevant question is whether the

officer reasonably believed that the warrant was properly issued, not whether probable cause existed in fact." *Id.* at 487 (quoting *United States v. Laughton*, 409 F.3d 744, 752 (6th Cir. 2005) (emphasis in original)). The good faith exception does not apply in four situations:

(1) where the issuing magistrate was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard for the truth; (2) where the issuing magistrate wholly abandoned his judicial role and failed to act in a neutral and detached fashion, serving merely as a rubber stamp for the police; (3) where the affidavit was nothing more than a "bare bones" affidavit that did not provide the magistrate with a substantial basis for determining the existence of probable cause, or where the affidavit was so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable; and (4) where the officer's reliance on the warrant was not in good faith or objectively reasonable, such as where the warrant is facially deficient.

Id. at 484 (citing *Leon*, 468 U.S. at 923).

Just last month, the Supreme Court of Florida refused to apply the good faith exception to the exclusionary rule after finding that officers violated the Fourth Amendment by tracking a suspect's location in real time. *Tracey v. State*,--- So. 3d ---, 2014 WL 5285929, at *20 (Fla. Oct. 16, 2014). But in that case, the police obtained only an order authorizing the installation of a pen register and trap-and-trace device on the defendant's cell phone, not a search warrant for real time cell site location information.

In *United States v. Fisher*, 745 F.3d 200 (6th Cir. 2014), the Sixth Circuit held earlier this year that the exclusionary rule did not apply to the warrantless GPS tracking of a vehicle that occurred (as here) before the Supreme Court decided *United States v. Jones* in 2012. The court found that the good faith exception applied because, at the time of the disputed GPS surveillance, the Supreme Court had not yet decided *Jones*, and "the Sixth Circuit and three other circuits had held, that the warrantless use of electronic tracking devices was permissible." *Id.* at 203. Although citing other cases, the court relied most heavily on *United States v. Forest*.

Neither *Forest* nor *Fisher* directly answers the good faith question here, as both of those cases involved "sporadic[]" tracking on public roads only. In this case, the police tracked White for multiple months on a continuous basis, on public roadways *and* in the privacy of his own home. And at the time the police tracked White, there was no Sixth Circuit precedent allowing officers to engage in warrantless electronic surveillance in areas protected by the Fourth Amendment. *See Davis*, 131 S. Ct. at 2435 (Sotomayor, J., concurring) ("Whether exclusion would deter Fourth Amendment violations where appellate precedent does not specifically authorize a certain practice and, if so, whether the benefits of exclusion would outweigh its costs are questions unanswered by our previous decisions."). Nonetheless, the police officers had obtained search warrants for the tracking activity, and they reasonably relied on the magistrate's determination that probable cause existed to track White's location by means of his cell phone.

District courts must generally accord "great deference" to a magistrate's determination, unless there is good reason not to do so. *United States v. Allen*, 211 F.3d 970, 973 (6th Cir. 2000) (en banc). No such reason exists here. The defendant has not argued — and the record does not show — that the police officers' affidavits contained false or reckless information. Nor is there any evidence that the magistrate acted as a rubber stamp for police activities or that the affidavits were facially invalid. It is a closer call as to whether officers could believe reasonably that probable cause existed. "An officer's belief that there is a sufficient nexus between the suspected crime and the place to be search is unreasonable when evidence in the affidavit connecting the crime to the residence is 'so vague as to be conclusory or meaningless." *United States v. Frazier*, 423 F.3d 526, 536 (6th Cir. 2005) (quoting *United States v. Carpenter*, 360 F.3d 591, 596 (6th Cir. 2004)). But an officer's good faith reliance on a warrant to conduct a search is reasonable if the "affidavit

contained a minimally sufficient nexus between the illegal activity and the place to be searched . . . even if the information provided is not enough to establish probable cause." *Carpenter*, 360 F.3d at 596.

The affidavit here does not contain any information to tie the illegal activity to a particular place: the affidavit requested the ability to track White on an ongoing basis on the assumption that wherever White traveled would lead to evidence of criminal activity. The breadth of the agents' electronic surveillance, as discussed already, amounted to an exploratory search prohibited by the Fourth Amendment. However, at the time that the magistrate issued the search warrants, there was no binding authority articulating the standard for establishing probable cause to obtain real-time cellsite location data. Neither the Supreme Court nor the Sixth Circuit has stated whether a warrant is required to obtain real-time cell-site data, and, if a warrant is required, whether probable cause demands that the government "show more than that the person is suspected of a crime." *Powell*, 943 F. Supp. 2d at 779. In the absence of such authority, officers here were prudent in first obtaining a warrant before tracking White, see Leon, 468 U.S. at 913 ("we have expressed a strong preference for warrants and declared that 'in a doubtful or marginal case a search under a warrant may be sustainable where without one it would fall.") (quoting *United States v. Ventresca*, 380 U.S. 102, 106 (1965)), and they reasonably relied on the magistrate's conclusion that probable cause existed. There is no evidence that officers acted with deliberate indifference, recklessness, or gross negligence in relying on the magistrate's conclusion that probable cause existed to obtain real-time cell-site location data from White's cell-phone. The good-faith exception to the exclusionary rule applies and suppression of the evidence will not be ordered.

V.

White argues that the evidence obtained from the search of his home is derived from the information obtained illegally from the original tracking warrant. The exclusionary rule is supplemented by the "fruit of the poisonous tree" doctrine, which bars the admissibility of evidence that police derivatively obtain from an unconstitutional search or seizure. *United States v. Pearce*, 531 F.3d 374, 381 (6th Cir. 2008) (citing *Wong Sun v. United States*, 371 U.S. 471, 484-85 (1963)). Because all of the evidence obtained from the original tracking warrants is admissible under the good faith exception, the warrant to search the house is not based on any tainted material that would require suppression under this doctrine. *See Powell*, 943 F. Supp. at 784.

Moreover, the evidence seized at White's home was discovered because of intercepted cell phone calls under a different, valid warrant, which was a source independent from the tracking warrants. "The exclusionary rule forbids the government from using evidence *caused* by an illegal seizure, not evidence found around the time of a seizure." *United States v. Figueredo-Diaz*, 718 F.3d 568, 576 (6th Cir. 2013) (internal citations and quotations omitted). Evidence should not be excluded if the police had an independent source for discovery of the evidence. *United States v. Akridge*, 346 F.3d 618, 623 (6th Cir. 2003).

The search warrant for White's home describes the history and content of certain intercepted calls from the wire intercepts that demonstrate a connection between White's drug trafficking and his residence. *See* dkt. #84-1 at 5 ("This affidavit contains information obtained through intercepted communications occurring over a cellular telephone utilized by WHITE II and surveillance in conjunction to these communications."). Although the affidavit also describes information obtained from tracking surveillance, *see id.* at 9-10, the information from the intercepted calls provided a sufficient and independent basis for the search warrant. A DEA agent listened to White make

multiple drug transactions over the phone from his cell phone, learned that his cell phone was

registered at the Baldwin Street address, and observed White at the address.

The intercepted calls furnished an independent source for the search warrant. There is no

basis to suppress the evidence seized from White's house.

V.

The cell site and GPS tracking evidence was seized illegally, but suppression may not occur

because the officers acted in good faith. The evidence seized from White's house was not obtained

in violation of the Fourth Amendment.

Accordingly, it is **ORDERED** that the defendant's motion to suppress evidence [dkt. #77]

is **DENIED**.

s/David M. Lawson

DAVID M. LAWSON

United States District Judge

Dated: November 24, 2014

PROOF OF SERVICE

The undersigned certifies that a copy of the foregoing order was served upon each attorney or party of record herein by electronic means or first

class U.S. mail on November 24, 2014.

s/Susan Pinkowski

SUSAN PINKOWSKI

-27-