CELLULAR-SITE AND IMPLICATIONS TO SEARCH AND SEIZURE UNDER THE 4TH AMENDMENT

E. Jay Abt, Esq. *

* A special thank you to Mazen Jabakhanji for his assistance in research and writing this article.

INTRODUCTION

Evidence obtained through a criminal defendant's cellular phone has been a hot legal topic since the rise of data technology in the 2000's. Unsure about the legal implications, police officers and law enforcement were generally handling seizures of cell phones as searches incident to arrest. Until 2014, police handled the searching and seizing of cell phones the same way they would handle purses, bags and packs of cigarettes; in conformity to case-law that allows searches incident to arrest. In 2014, the Supreme Court ruled that, absent a search warrant, the searching of cell phones during a routine stop is prohibited under the 4th amendment. See Riley v. California, 134 S. Ct. 2473 (2014). After Riley, prosecutors and law enforcement began looking at other means of obtaining information in cell phones without having to actually obtain a physical phone or it's data. The federal government began obtaining information regarding a cell phone's contents and whereabouts, or metadata, through cell phone towers. This information was obtained through a federal statute that requires "wireless providers", such as T-Mobile or MetroPCS, to disclose customer records or communications, that the provider holds for 180 days, at the request of the government. 18 U.S.C. §2703. These records of information, known as cell-site data show, inter alia, GPS coordinates of cell phones that were used during a certain time. Cell-site data can also be used by triangulating the phone's location using either the *time difference of arrival* or *angle of arrival techniques*.

In a recent 6th Circuit Court of Appeals case, the central issue was whether the Government can simply obtain this type of metadata without a search warrant. United States v. Carpenter, 819 F.3d 880 (6th Cir. 2016). The 6th Circuit, which presides over cases in MI, OH, KY and TN, ruled that the metadata is comparable to mailing addresses, phone numbers, and IP

addresses where the information being obtained is not the communications itself but rather *public* data that goes along with it. The U.S. Supreme Court granted a review of Carpenter and heard oral argument on November 29, 2017, but there is no published decision in the case yet.

There are major cases that brought about the issue of metadata and cell-site data, and how courts have justified their decisions since Riley regarding cell phone data. Analyzing the process of how cell site data is collected and the arguments for and against the expectation of privacy regarding geographic data is relevant to explain how law enforcement uses this data in furtherance of building evidence while investigating a suspected criminal defendant.

THE RILEY EFFECT

In August 2009, David Riley was pulled over in San Diego, California for having expired tags on his car and a suspended driver's license. As per police department policy, the officer impounded Riley's car and conducted a warrantless search of the car. The officer found two handguns that were later linked to a shooting that had taken place a few weeks prior. During the arrest, the officers confiscated and went through the data on Riley's smartphone without a warrant. Some of the data on the phone linked Riley to gang activity and the shooting, and was entered into evidence at the trial, where Riley was convicted on three charges. Riley argued that allowing police officers to search through data on his cell phone without a warrant is an unacceptable intrusion on personal privacy. California argued that police officers need to be able to confiscate cell phones without first obtaining a warrant for safety reasons and to prevent destruction of evidence.

The Supreme Court ruled in Riley v. California in 2014 that police officers generally must secure a warrant before conducting a search of the contents of a cell phone seized incident

to an arrest. The search of a person incident to an arrest is, among other exceptions, a valid exception to the warrant requirement of the Fourth Amendment. This exception is permitted for the safety of the arresting officer and to prevent destruction of evidence. Chimel v. California, 395 U.S. 752 (1969). The Court believed that there is no safety risk to a police officer other than if the phone has a blade or weapon hidden in its battery compartment or something of that sort. The Court also believed that there is minimal risk of destruction of evidence stored on the phone through remote wiping or encryption, and therefore goes beyond the concern in Chimel that a defendant can destroy whatever is within reach. The Court continued to argue that unlike the pack of cigarettes in Chimel where police officers are allowed to search without a warrant, a cell phone actually contains personal information just as sensitive as that which a regular person would store in his home. Of course, law enforcement would be required to obtain a search warrant in pursuance of searching one's home. The government argued that, pursuant to Arizona v. Gant, 556 U.S. 332 (2009), a warrantless search of a cell phone is justified when the cell phone is reasonably believed to contain evidence of the crime of arrest. Gant applied to searches of vehicles, however, and the search of a cell phone cannot possibly be limited in any reasonable fashion. In conclusion, the Court ruled that the government must obtain a search warrant prior to searching a cell phone's contents.

After Riley, law enforcement began obtaining warrants in order to search cell phones that were incident to an arrest. Headnote 8 of Riley, which says that warrants must be obtained prior to the searching of cell phones, is cited to about eighteen times in Federal Circuit Courts since 2014. The bulk of these cases do not introduce new issues regarding the substance of searches but rather procedural issues not worth pursuing with regards to this paper Chatman v. Green, No. PWG-15-2827, 2016 U.S. Dist. LEXIS 52326 (D. Md. Apr. 18, 2016); Cantu v. Platinum Mktg.

Grp., LLC, No. 1:14-CV-71, 2015 U.S. Dist. LEXIS 90824 (S.D. Tex. July 13, 2015); United States v. Gardner, No. 16-cr-20135, 2016 U.S. Dist. LEXIS 128480 (E.D. Mich. Sep. 21, 2016); Sollenberger v. Sollenberger, 173 F. Supp. 3d 608 (S.D. Ohio 2016); United States v. Thurman, No. 14 CR 366, 2017 U.S. Dist. LEXIS 21497 (N.D. Ill. Feb. 15, 2017). Thurman states that although a search warrant is required prior to the search of cell phones, a voluntary consent basically waives the requirement for the warrant. Id. at Thurman.

In addition to obtaining warrants prior to the search of cell phones, law enforcement began seeking other avenues in locating suspects that were being investigated. Law enforcement started going back to the actual data that was being emitted from the cell phone, metadata, and using that as a way of not only tracing communications and its contents, but rather locating the live location of the cell phone itself. Naturally, defense lawyers have argued that this metadata is not public information and as a result, is illegally obtained absent a search warrant.

UNITED STATES v. CARPENTER

Cellphones work by establishing a radio connection with nearby cell towers (or "cell sites") and those phones are constantly searching for the strongest signal from those towers. Individual towers project different signals in each direction or "sector," so that a cellphone located on the north side of a cell tower will use a different signal than a cellphone located on the south side of the same tower. Cell towers are typically spaced widely in rural areas, where a tower's coverage might reach as far as 20 miles. In an urban area however, each cell site covers typically anywhere from a half-mile to two miles. Wireless carriers typically log and store certain call-detail records of their customers' calls, including the date, time, and length of each call; the phone numbers involved on the call; and the cell sites where the call began and ended.

See United States v. Carpenter, 819 F.3d 880 (6th Cir. 2016). This information is called "cell-site" data and is the center of an ongoing dispute in Federal Courts.

Carpenter is the highlighted 6th Circuit Court of Appeals case regarding the obtaining and use of cell-tower or "cell-site" data by law enforcement. In April 2011, Detroit police arrested four men suspected of committing a string of armed robberies at Radio Shacks and T-Mobile stores in and around the Metro-Detroit area. After the arrest, one of the four men confessed that the group had robbed nine different stores in Michigan and Ohio between December 2010 and March 2011, supported by 15 other men who served as getaway drivers and lookouts during these robberies. The robber who confessed to the crimes gave the FBI his own cellphone number and the numbers of other participants; the FBI then reviewed his call records to identify more numbers that he had called around the time of the robberies. In May and June 2011, the FBI applied for three orders from magistrate judges to obtain "transactional records" from various wireless carriers for 16 different cell phone numbers. As part of those applications, the FBI said that these records included "all subscriber information, toll records and call detail records including listed and unlisted numbers dialed or otherwise transmitted to and from the target telephones from December 1, 2010 to present" as well as "***cell site information*** for the target telephones at call origination and at call termination for incoming and outgoing calls". The magistrate judges granted the applications pursuant to the Stored Communications Act, codified at 18 U.S.C. §§ 2701–2712, under which the government may require the disclosure of certain telecommunications records when "specific and articulable facts show that there are 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." 18 U.S.C. § 2703(d).

Before trial, defendants Carpenter and Sanders moved to suppress the government's cell-site evidence on Fourth Amendment grounds, arguing that the records could only be seized with a warrant supported by probable cause. The district court denied that motion.

With the cell-site data provided by Carpenter's and Sanders's wireless carriers, the FBI created maps showing that Carpenter's and Sanders's phones were within a half-mile to two miles of the location of each of the robberies around the time the robberies happened. The FBI then used MetroPCS call-detail records to show that Carpenter was within that proximity of a Detroit Radio Shack that was robbed around 10:35 a.m. on December 13, 2010. Specifically, MetroPCS records showed that at 10:24 a.m. Carpenter's phone received a call that lasted about four minutes. At the start and end of the call, Carpenter's phone drew its signal from MetroPCS tower 173, sectors 1 and 2, located southwest of the store and whose signals point north-northeast. After the robbery, Carpenter placed an eight-minute call originating at tower 145, sector 3, located northeast of the store, its signal pointing southwest; when the call ended, Carpenter's phone was receiving its signal from tower 164, sector 1, alongside Interstate 94, just north of the Radio Shack at issue.

This evidence presented by the government led the jury to convict Carpenter and Sanders. The Defendants then appealed their convictions and sentences to the 6th Circuit Court of Appeals in 2016.

In the 6th Circuit, the court disagreed that cell-cite data was protected under the 4th amendment due to a reasonable expectation of privacy. The 6th Circuit argued that although the content of personal communications is private, the information necessary to get those communications from point A to point B (cell-site data) is not. The 6th Circuit cited to the Supreme Court holding in Ex parte Jackson where the Court held that postal inspectors needed a

search warrant to open letters and packages, but that the "outward form and weight" of those mailings—including the recipient's name and physical address—was not constitutionally protected. Ex parte Jackson, 96 U.S. 727, 733, 24 L. Ed. 877 (1878). Although the Court recognizes that a search warrant is needed in order to eavesdrop on a phone call, in Smith, the Court held that the police's installation of a pen register, a device that tracked the phone numbers a person dialed from his home phone—was not a search because the caller could not reasonably expect those numbers to remain private. Although the caller's conduct may have been calculated to keep the contents of his conversation private, his conduct was not and could not have been calculated to preserve the privacy of the number he dialed. Smith v. Maryland, 442 U.S. 735, 740, 99 S. Ct. 2577, 61 L. Ed. 2d 220 (1979).

The 6th Circuit held that the Carpenter records say nothing about the content of any calls. Instead the records include routing information, which the wireless providers gathered in the ordinary course of business. Cell phone carriers necessarily track their customers' phones across different cell-site sectors to connect and maintain their customers' calls. Carriers keep records of this data to find weak spots in their network and to determine whether roaming charges apply, among other purposes. Thus, the cell-site data—like mailing addresses, phone numbers, and IP addresses—are information that facilitate personal communications, rather than part of the content of those communications themselves. Accordingly, the 6th Circuit held that the government's collection of business records containing these data therefore was not a search and required no search warrant. The Supreme Court has now heard the appeal and a decision is pending.

EXPECTATION OF PRIVACY IN GEOLOCATION DATA

With respect to cell site data, another key question for courts to answer is whether a criminal defendant has a reasonable expectation of privacy in cell phone data that broadcasts their location. In the same 6th Circuit that ruled on Carpenter last year-- that court ruled no, a defendant did not enjoy that expectation of privacy. See United States v. Skinner, 690 F.3d 772, 777 (6th Cir. 2012) (holding that the defendant did not have a reasonable expectation of privacy in location data broadcasted from his cell phone). In Skinner, law enforcement used data stemming from defendant's pay-as-you-go cell phone to determine its real-time location as he transported drugs along public highways. The agents located the defendant at a rest stop, with a motorhome filled with marijuana. The appellate court determined that the suppression of the data was not warranted because there was no Fourth Amendment violation since defendant did not have a reasonable expectation of privacy in the GPS data and location of his cell phone because authorities tracked a known number that was "voluntarily" used. The court also found that no extreme comprehensive tracking was present in this case. It is reasonable to conclude that this court's reasoning was that people voluntarily choose the network carriers based on an open market, sign an agreement to have the data that emits from those phones to be public, and voluntarily carry the phones on their persons at all times the phone is with them.

In addition to Skinner, the Northern District of Mississippi agreed in 2015 with a similar question presented in Skinner but this time, not for previous data, but for future prospective data. See *In re Application of the United States of America for an Order for Authorization to Obtain Location Data Concerning an AT&T Cellular Tel.*, 102 F. Supp. 3d 884, 2015 U.S. Dist. LEXIS 56241, 2015 WL 1842761, at *6 (N.D. Miss. Mar. 30, 2015) (holding that suspects did not have a reasonable expectation of privacy in location data transmitted from their cell phones). In this

case, law enforcement was seeking an order from a magistrate judge to allow the surveillance and obtainment of data from cell-towers for ***future*** dates. Although this was a departure from the previous issues regarding past data, this was a question for ***future data***. The court held, in accordance with other case law, that a defendant simply does not have a reasonable expectation of privacy in location data transmitted from cell phones. It is also important to note this courts admission that there is simply no Supreme Court precedent to follow and thus, courts would need to use their discretion until such question is answered in a higher court. "In the absence of relevant U.S. Supreme Court authority, lower federal courts have analyzed the constitutional issues in this context in different ways". Id. at In re application. In other words, it is reasonable to believe that this court, like many other courts deciding on this issue, are waiting for Carpenter as a reference to rule on similar issues in the future.

The case of Lang adds to the analysis in Skinner. United States v. Lang, 78 F. Supp. 3d 830, 2015 WL 327338, at *4 (N.D. III. 2015) (an individual does not have a legitimate expectation of privacy in historical cell site information and thus the protections of the Fourth Amendment do not apply). Similar to the holding in Skinner, the defendant argued that the federal government did not have the right to search the contents of cell-site data absent a warrant. Thus, a search warrant was not required in Lang.

The 2013 Eastern District of New York case regarding prospective and future geolocation data assists these courts' analysis. See In re Smartphone Geolocation Data Application, 977 F.Supp.2d 129, 147 (E.D.N.Y. 2013) (holding that cell phone users who fail to turn off their devices do not have a reasonable expectation of privacy regarding prospective geolocation data and such expectation would not be reasonable in any event). In that case, a magistrate judge held that where the government demonstrated probable cause to believe that prospective geolocation

data would aid in a defendant's conviction, a court was allowed to issue a search warrant to authorize access to such data. The court also ruled that a defendant has no reasonable expectation of privacy in prospective cell-site data where cell phone users agreed with their telecommunication carrier and smartphone manufacturer, upon buying and activating it, that their geolocation information could be tracked and provided without consent. Prior to activating a cell phone with a carrier, the carrier requests the user to sign, what is often referred to as an "adhesion contract", which is boilerplate, take it or leave it language, but in voluminous small print that no reasonable consumer or private individual would bother to read. In such an agreement, there is a clause that states that the user's geolocation information and/or data could be tracked and provided without that user's consent. The government in this case did not need to obtain a search warrant to use geolocation data to find the defendant as the issuance of an arrest warrant undermined any expectation of privacy. Finally, the government could properly seek an authorization order for prospective cell data under § 2703 as a cell phone did not fall within the tracking device exclusion of § 3117 Mobile Tracking Devices.

In an instructive case, Barrera, a suspected cocaine drug-dealer was convicted based on cell-ping information obtained by the DEA Drug Task Force. United States v. Barrera-Barron, 2013 U.S. Dist. LEXIS 108410, 2013 WL 3989182, at *4 (D. Kan. Aug. 1, 2013) (the defendant did not have a reasonable expectation of privacy in the GPS data from the cell phone that was used to track his whereabouts, thus he lacked standing to contest the use of that data). In this case, the DEA agent obtained a GPS location based on a cell phone ping. This ping eventually led to the whereabouts and the arrest of the defendant. The defendant moved to suppress the evidence because he argued that his GPS data was protected under the 4th amendment. The court

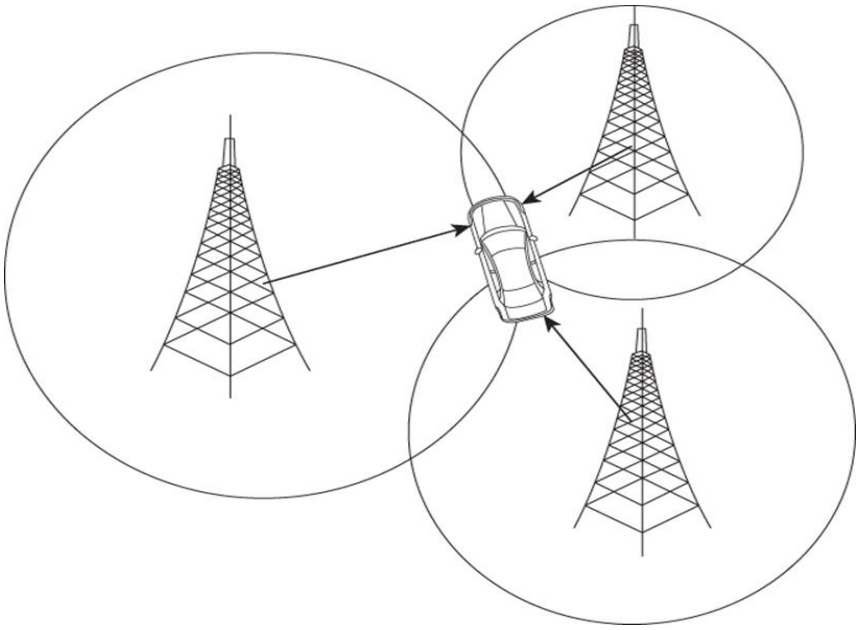
sharply disagreed with the defendant and argued instead that the GPS data was public information.

An emerging pattern can be observed with the federal courts leaning in favor of government use of technology to combat crime, rather than protecting individual and civil liberties. In particular lower and appellate federal courts, outside the scope of Riley, have trended to allow the government to access, use and admit evidence that technology in an emerging society becomes easier to obtain. These decisions act at the expense of any expectation of or actual privacy regarding cell-tower data. As a result, almost every federal court has argued that this sort of data, while may be seen as private, is indeed public information and thus, would not require law enforcement to obtain search warrants in order to gain that information. In turn, law enforcement uses a range of techniques in order to "map out" the information which basically provides them with the location or an estimate of where a certain individual may have been at the time the data was emitted from their cell phone. This technique is called, among others, "cell-data triangulation".

CELL DATA TRIANGULATION

Cell phone towers get information regarding a cell-phone user's location in two ways: using GPS technology, or by triangulating the phone's location using either the *time difference of arrival* or *angle of arrival techniques*. Cell phone networks are broken up into coverage areas, knows as "cells" which range in coverage diameter depending if the location is in a rural or urban location. The more urban the location, the greater the number of cells and thus the easier to locate the cell phone. When a person turns on a cell phone, it periodically sends a signal to all the towers within its range. The time distance of arrival method basically tracks a phone's points of longitude and latitude when a communication is sent or received, and a triangulation algorithm

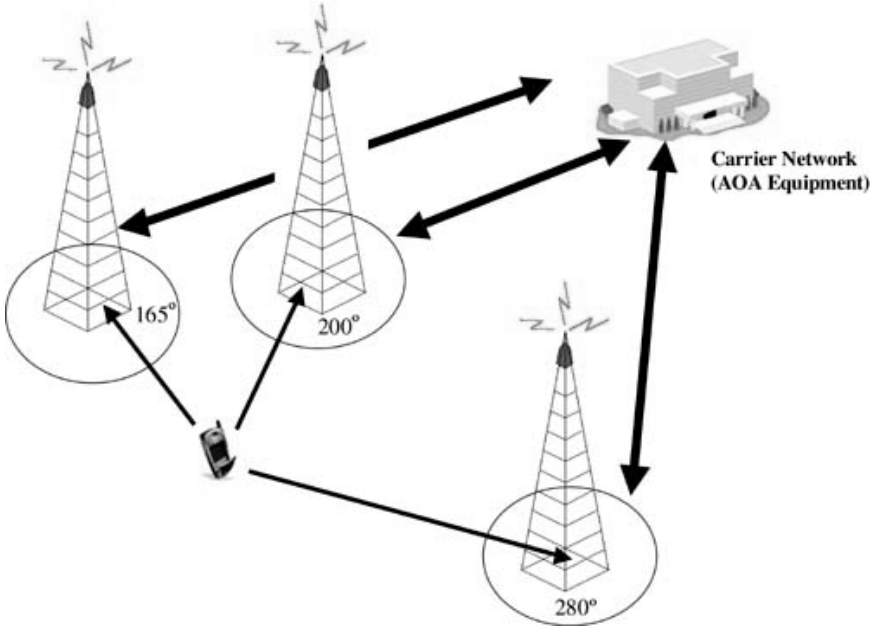
or “pattern” produces an estimate of the phone’s location by measuring the time it takes for different cell towers’ signals to reach the phone. For example, if cell tower 100’s time is significantly lower than tower 101 and 102, it is safe to assume that the phone is near or closer to the cell of tower 100.



The time of arrival technique takes the time of the signal received and sent from each tower, then it uses an average of that time in order to try to pinpoint where that signal derived from (the cell phone). This assists law enforcement if they are searching for a phone or have a general question as to where that phone was at a certain time and date. If the data in that tower states that the phone was not there at all at a time in question, then it may be safe to assume that the suspected criminal was not present at that time. But an important scientific question is also raised as to the accuracy of the triangulation, which can and should be disputed.

Alternatively, the angle of arrival method uses the angles of the signals, rather than measuring the time it takes for those signals to go and come back, to figure out the location of that phone. The accuracy of this method however, rests on how many cell-towers were within the

range (urban or rural). For an accurate estimate, whatever that may mean, data stemming from at least three towers is sufficient.



Although in some situations, such as in rural scenarios, three towers may not exist; the frequency from two towers may still be able to establish an estimate of a cell phone's location at a certain time.

CONCLUSION

In a post Riley world, technology and cellular data continues to develop at rapid pace. Law enforcement appears to understand the holding in Riley, and the need to obtain search warrants for the data located on an individual phone. However, an increasing trend exists that the data which that phone sends or receives to any 3rd party location, whether it be another phone, a cell phone tower, or a carrier's records, will not contain any expectation of privacy protected by the 4th Amendment. Moreover, cellular data is not protected if it is historical or prospective future data, if a the government can access the data from a 3rd party, without the necessity of a warrant.