FDCC CIVIL "WRITES"

A monthly newsletter from the Civil Rights and Public Entity Committee

January, 2025 - Editor of the Month Jeff Lowe

Happy New Year to all Section Members. I hope your year has started well and you are well on your way to completing all your New Year's resolutions. The month's edition addresses issues that may arise if your officers use a suspect's real-time cellular data to locate and apprehend that suspect.

ISSUE OF THE MONTH – POLICE OFFICERS' USE OF REAL-TIME CELLULAR DATA TO LOCATE SUSPECTS

I recently ran into an issue that I found interesting and thought might be of benefit to fellow Section members. Short story is officers used a suspect's cellular telephone name and number to send a request to the suspect's provider for real-time cellular location data to locate the suspect and a juvenile runaway who was believed to be suicidal and potentially being taken advantage of by the suspect. The officer's used the form provided by the provider to request that data which states that pursuant to 18 U.S.C. 2702(b)(8) or 2702(c)(4), the provider may divulge records or other information to governmental entities in certain emergencies. The officers did not seek a search warrant to obtain the information. The officers made the request, the provider provided information that allowed the officers to communicate with authorities in another state to locate the subject and the juvenile runaway. The suspect was arrested, tried and convicted and subsequent to the conviction sued the officers who requested the cellular data for violations of his 4th Amendment rights and a violation of the Federal Wiretap Act.

As to the Fourth Amendment claim, you may be asking whether a cellular customer has a reasonable expectation of privacy in the real-time cellular telephone data. In June 2018, the United States Supreme Court in *Carpenter v. United States*, 585 U.S. 296, held law enforcement officials must generally obtain a warrant before obtaining historical cell-phone location data, but left open the question of whether the same rule governed law enforcement's efforts to obtain real-time cellular data. The Seventh Circuit addressed that particular issue in *United States v. Hamilton*, 996 F.3d 374 (7th Cir 2021). It held the criminal defendant in that case had no reasonable expectation of privacy in his real-time cellular data that officers used to track his movements over public roads and streets. The Seventh Circuit distinguished the *Carpenter* decision's rationale based on several factors, including that the officers were only monitoring his location by real-time cellular data for several hours as opposed to the 127 days of historical data in *Carpenter* and the collected location data only showed what the suspect exposed to public view while he travelled on public interstate highways and into parking lots. Further, the Seventh Circuit held the retrospective nature of the surveillance in *Carpenter* was not present in Hamilton's case and society was not prepared to recognize that law enforcement could not surveil someone over the course of several hours on public roads through other methods such as tailing someone or through a stake out. Thus, the Seventh Circuit held the Detective did not conduct a Fourth Amendment search by requesting real-time cellular data of a suspect for multiple armed robberies for whom officers had probable cause to arrest when they only collected the data for a matter of hours while the suspect travelled on public roads and law enforcement limited its use of the cellular data to the purpose of finding the armed suspect who they had reason to believe may commit another armed robbery. The court found Hamilton's expectation of privacy was not one society was prepared to recognize as reasonable, but noted its holding was narrow and limited to the facts of that case.

It should be noted that there is a split among circuits and state courts regarding whether law enforcement's use of real-time cellular data is a search for 4th Amendment purposes. In *United States v. Baker*, 563 F.Supp.3d, 361 (M.D. Pa. 2021) a federal district court in Pennsylvania distinguished *Hamilton* and found law enforcement's use of real-time cellular data was a search because it pinpointed the

criminal defendant in his home and the 4th Amendment's protections in one's home supported the defendant's reasonable expectation of privacy. The court in *Baker*, however, held the exigent circumstances exception to the warrant requirement justified the warrantless search. California, Kentucky, and Rhode Island have also held use of real-time cellular data constitutes a search under the 4th Amendment.

Therefore, until the Supreme Court addresses the use of real-time cellular data in a 4th Amendment context, there seems to be a split of authority regarding whether a person has a reasonable expectation of privacy in that person's real-time cellular data. Certain factors that have been found to favor a reasonable expectation of privacy are that the person was located in their home at the time law enforcement recovered the data. Factors courts have used to not find a person has a reasonable expectation of privacy in real-time cellular data have been the length of time law enforcement received and used the data and using the data to surveil someone outside of their home. Even if officers do not obtain a warrant and there exists a reasonable expectation of privacy in your jurisdiction, the standard exceptions to the 4th Amendment warrant requirement apply to this situation and can obviate the need for a warrant. Additionally, qualified immunity would potentially protect your officers if there is a lack of clarity in your circuit regarding the circumstances in which cellular telephone customers have a reasonable expectation of privacy in their real-time cellular phone data.

Law enforcement could avoid any question by applying for and receiving a warrant to obtain the real-time cellular data, but making that request opens a lot of other issues regarding whether a cell phone is a tracking device and what is the proper standard for the reviewing Magistrate to apply to determine whether to authorize the retrieval of real-time cellular data.

Specifically, the case of *U.S. v. Bermudez,*2006 WL 3197181 (S. D. Ind. June 30, 2006) is instructive. There, the government sought and obtained an order authorizing the receipt of cellular site information from a target phone pursuant to the Stored Communications Act (18 U.S.C. §2701 et seq.) and the Pen/Trap Act (18 U.S.C. §3121 et seq.). The criminal defendant contended the warrant exceeded the limitations imposed by those statutes and the proper standard for issuance of the warrant was Federal Rule of Civil Procedure 41 and 18 U.S.C. §3117 which both require a finding of probable cause before the court can issue a warrant or other order for the

installation of a mobile tracking device. The court began its analysis by explaining the relevant technology as follows:

> When powered on, a cell phone is (among other things) a radio transmitter that automatically announces its presence to a cell tower or "cell site" via a radio signal over a control channel which does not itself carry the human voice. *In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority,* 396 F.Supp.2d 747, 751 (S.D.Tex.2005) [hereinafter *Texas Cell Site Case*].[16] The phone is constantly seeking the best reception, re-scanning for cell sites every seven seconds or when the signal strength weakens, regardless of whether a call is made. *In re Application of U.S. 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, 599 (D.Md.2005) [hereinafter *Maryland Cell Site Case].* "Real time" cell site information refers to data available to and used by the government to identify the location of a phone at a given moment. The use of real time cell site information by law enforcement for tracking purposes is a relatively new law enforcement tool and Congress has yet to provide specific legislative boundaries on the practice. Therefore, we analyze the disclosure of real time cell site information under the existing more generalized statutory scheme. *Id.*

The court then discussed the Electronic Communications Privacy Act of 1986 (ECPA) to determine the proper statutory framework to evaluate the defendant's motion to suppress. The ECPA has three titles, Title I governing tracking devices, Title II governing stored electronic information and Title III governing pen register and trap and trace devices. Analyzing the purposes and statutory language of Titles II and III, the Court determined they did not apply, and Title I provided the proper framework for analysis of the defendant's question.

Specifically, with regard to Title II, the Stored Communications Act part of the ECPA, the court found the core purpose of that Title was to authorize the government to require disclosure of stored communications and transaction records by third party service providers. The court found the disclosure of real-time cell-site data is not covered by the first two types of records protected by the SCA because it did not

involve contents of the conversations. The court also found the third type of information protected by the SCA, "stored communications," does not include real-time cell-site information. Therefore, the Court found the magistrate's reliance on the SCA to issue the warrant was not justified and did not authorize receipt and use of the real-time cell site information under the ECPA.

With regard to Title III, the Pen/Trap Act, the court held the statute authorizing Pen/Trap warrants specifically excludes information that may disclose the physical location of the subscriber, and therefore the warrant for real-time cell site information could not be supported by that statute.

Turning to Title I of the ECPA, the court found:

> Title I of the ECPA amended the 1968 federal wiretap statute (the "Wiretap Act") to include electronic communications, providing that, before a telephone conversation can be lawfully intercepted, there must be a judicial determination of probable cause. *See generally* 18 U.S.C. § 2518; *Texas Cell Site Case,* 396 F.Supp.2d at 751. One portion of ECPA's Title I expressly relates to mobile tracking devices. Pub.L. No. 99-508, Title I, § 108(a), 100 Stat. 1858 (Oct. 21, 1986) (codified at 18 U.S.C. § 3117). These provisions authorize a court "to issue a warrant or other order for the installation of a mobile tracking device" which may move across district lines. 18 U.S.C. § 3117(a). The term "tracking device" is broadly defined to mean "an electronic or mechanical device which permits the tracking of the movement of a person or object." 18 U.S.C. § 3117(b). As noted in the *Texas Cell Site Case,* the tracking device statute "does not distinguish between general vicinity tracking and detailed location tracking." 396 F.Supp.2d at 755. Instead, the statute simply defines a tracking device as "an electronic or mechanical device which permits the tracking of the movement of a person or thing." 18 U.S.C. § 3117(b). "[C]ell-site data unquestionably permits the tracking of the movement of a cell phone when two-thirds of users can be pinpointed within 100 meters and 95 percent within 300 meters." *Maryland Cell Site Case,* 402 F.Supp.2d at 603-04. Moreover, "the Department of Justice itself uses the term 'tracking device' to describe a device that acquires 'information that will allow [a mobile telephone] properly to

> transmit the user's voice to the cell tower' and thereby determine 'the direction and signal strength (and therefore the approximate distance) of the target phone.' " *New York Cell Site Case,* 396 F.Supp.2d at 310 - 311; (*quoting Texas Cell Site Case,* 396 F.Supp.2d at 755 n. 12, and U.S. Dep't of Justice, Electronic Surveillance Manual at 45 (rev. June 2005)).
>
> Unlike other provisions in the ECPA, Title 18 U.S.C. § 3117 does not contain any direction to law enforcement or standards for obtaining a warrant permitting the installation of and monitoring by a tracking device. *Maryland Cell Site Case,* 402 F.Supp.2d at 604. Because the ECPA was not intended to affect the legal standard for the issuance of orders authorizing these devices, *see* 752 H.R. Rep. 99-647, at 60 (1986), a Rule 41 probable cause showing and procedures were (and still are) the standard procedure to authorize the installation and use of mobile tracking devices. *See United States v. Karo,* 468 U.S. 705, 720, 104 S.Ct. 3296, 82 L.Ed.2d 530 n. 6 (1984) (holding that warrantless monitoring of beeper in private residence violates Fourth Amendment); *see also Texas Cell Site Case,* 396 F.Supp.2d at 752. Like other Rule 41 warrants, the only limit on authorizing and conducting such searches (or in this case, electronic devices) is the Fourth Amendment. *See Maryland Cell Site Case,* 402 F.Supp.2d at 604. In other words, only if a Fourth Amendment privacy interest exists which would be violated by the government's mobile tracking of a cell phone, is a warrant necessary for the search.
>
> Our research has revealed no binding precedent in this circuit on the issue of whether a warrant based on probable cause is needed before the government can use cell site information to track a cell phone's location.

The court did not have the benefit of the *Hamilton* decision that now exists in the Seventh Circuit that there is no reasonable expectation of privacy in the real-time cellular site location data. However, not all courts treat this issue similarly and if you run into this issue, I would advise you to research the proper standard in your circuit to determine what the proper standard for the warrant is and whether a warrant is required in your circuit. The importance of determining whether the proper standard was applied and met is because it could determine whether your officers have violated the Federal Wiretap Act and improperly obtained electronic

communications of a suspect as case law seems to make clear that communications between a person's cellular phone to a cell tower are electronic communications protected by the Act.

HELP WANTED!

We are in need of, and want, new members to the Federation generally, and our Committee specifically. This includes greater diversity, more insurance professionals and in-house government lawyers. Please make an extra effort to nominate qualified candidates to join us.

We are also in need of: (1) volunteers to present at upcoming conferences and webinars; (2) writers to author articles for our publications; and (3) ideas for topics that would be of interest to our Committee members and/or the Federation. If you have any interest or ideas, please contact Nat or any of the Vice Chairs.