UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN RE: THE USE OF A CELL-SITE SIMULATOR TO LOCATE A CELLULAR DEVICE ASSOCIATED WITH ONE CELLULAR TELEPHONE PURSUANT TO RULE 41	**CASE NO. 20-SC-3276 (ZMF)**

ORDER

On December 20, 2020, the government submitted a Motion to Seal and for Delayed Notification ("Motion") as part of an Application for a Search Warrant ("Application"). The Application requested authority pursuant to Rule 41 of the Federal Rules of Criminal Procedure to use a cell-site simulator for 30 days in an effort to locate a specified cellphone number associated with a fugitive. *See* Appl., ECF No. 1. On December 23, 2020, the undersigned magistrate judge granted the application but denied the sealing request. *See* ECF No. 3-1. On December 26, 2020, the government filed an Amended Motion to Seal and for Delayed Notification ("Amended Motion"). *See* Mot., ECF No. 2; Am. Mot., ECF No. 3.[1] The Court again denied this request. On December 28, 2020, the government filed a Second Amended Motion to Seal and Delay Notification ("Second Amended Motion"). *See* Second Am. Mot., ECF No. 6. For reasons explained below, the undersigned granted the Second Amended Motion that same day. The order precluded recordation of the Application on the public docket (*i.e.*, sealing) and precluded immediate notification to the subject of the search (*i.e.*, delayed notice). *See id.* at 9–10.

[1] Both Applications erroneously referenced non-disclosure orders in their titles, yet the Applications themselves indicated that "[t]he service provider for the target cell phone is not required to produce records or provide assistance, so a non-disclosure order is not needed." Mot. 1, ECF 2; Am. Mot. 1, ECF No. 3.

I. Background

a. Cell-Site Simulators and Cell Phones

Cell-site simulators are relatively new devices that exploit a common cell phone function. When powered on, "[c]ell phones are designed to seek, identify, and connect with the cell [site] having the best signal in the area." *United States v. Johnson*, No. S1-4:18 CR 565-1 CDP (JMB), 2020 WL 6049562, at *13 (April 14, 2020 E.D. Mo.). The best signal "generally comes from the closest cell site." *Carpenter v. United States*, 138 S. Ct. 2206, 2211 (2018). These signals from cell sites connect cell phones to networks maintained by private cellular service companies. A cell-site simulator mimics the signaling function of a private cell site. Like a moth to the flame, a cell-site simulator emits signals causing nearby cell phones to "identify the simulator as the most attractive cell tower in the area and thus transmit signals to the simulator that identify the [simulator] in the same way that they would with a networked [cell site]." Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology (Sept. 3, 2015), at 2 [hereinafter DOJ Guidance].

The Department of Justice ("DOJ") states that cell-site simulators can serve two purposes: (1) "to help locate cellular devices whose unique identifiers are already known to law enforcement," and (2) "to determine the unique identifiers of an unknown device by collecting limited signaling information from devices in the simulator user's vicinity." *Id.* at 1. DOJ instructs federal agents to configure "[c]ell-site simulators [to] provide only the relative signal strength and general direction of a subject cellular telephone; they do not function as a GPS locator." *Id.* "If the [DOJ's] description is accurate . . . law-enforcement officials get the same sort of information that a phone company could provide using its own facilities, and they get it in real time rather than

waiting for the phone company to turn over data.[2] *United States v. Patrick*, 842 F.3d 540, 543 (7th Cir. 2016). Despite this limited use, DOJ directs prosecutors to "either (1) obtain a warrant that contains all information required to be included in a pen register order pursuant to 18 U.S.C. § 3123 (or the state equivalent), or (2) seek a warrant and a pen register order concurrently."[3] *See* DOJ Guidance at 3. The Application aligns with DOJ's prescribed guidance as it sought a "to comply with the Pen Register Statute as well as with Rule 41." Aff.6, ECF No. 1.

b. The Warrant

The Warrant authorized the government to use a cell-site simulator to "identify the location of the cellular device assigned phone number [REDACTED], whose wireless provider is T-Mobile and is believed by law enforcement to be used by [the fugitive, hereinafter the 'Subscriber']." Attach. A, ECF No. 1. The Warrant further authorized the government to "collect[] and examin[e] . . . radio signals emitted by the target cellular device for the purpose of communicating with cellular infrastructure [and those] in response to radio signals sent to the cellular device by the officers." Attach. B, ECF No. 1. The Warrant explicitly did not authorize "interception of any telephone calls, text messages, other electronic communications, and . . . prohibit[ed] the seizure of any tangible property." *Id.* The Application noted that the cell-site simulator "may interrupt cellular service of phones or other cellular devices within its immediate vicinity," but stated that the simulator "will not complete a connection with cellular devices determined not to be the Target Cellular Device . . . ." Aff. 21, ECF No. 1.

---

[2] Some judges and scholars worry that cell-site simulators may be more invasive. *See Patrick*, 842 F.3d at 547 (Wood, J., dissenting) (citing Stephanie K. Pell & Christopher Soghoian, *Your Secret Stingray's No Secret Anymore; The Vanishing Government Monopoly over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy*, 28 Harv. J.L. & Tech. 1, 11–12 (2014)).

[3] DOJ instructs federal agents to configure cell-site simulators as pen-register devices. *See* DOJ Guidance, *supra*, at 1.

The Application established that there was:

- probable cause to believe that the Subscriber was "actively evading arrest" due to his likely knowledge of the pending indictment and arrest warrant, Aff. 4, ECF No. 1;
- "reason to believe the Target Cellular Device [was] located somewhere within this district" at the time of the application, *id.* at 2; and
- probable cause that the Subscriber possessed a cell phone with the specified phone number and that the Subscriber was likely to be in possession of that cell phone when the government planned to use the cell-site simulator to locate it. *See id.* at 3, 9.

II. Requirements for Warrant Authorizing Cell-Site Simulator Use

When presented with the Application, the Court considered whether the use of a cell-site simulator for 30 days to locate a single cell phone belonging to a fugitive whose location is unknown constitutes a Fourth Amendment search.[4] For the reasons stated below, "the Fourth

[4] The Application "assume[d] that a search warrant is likely to be required to use a cell site simulator even though the device does not capture content of communications and even though the U.S. Supreme Court has not yet ruled that a warrant is required for use of this device." Aff. 4, ECF No. 1. The Application also stated that the cell-site simulator "does enable searchers to locate a cell phone without implementation of an actual mobile tracking mechanism and the Supreme Court rulings suggest that cell phone location is protected privacy under the Fourth Amendment." *Id.*

In authorizing the Warrant, the undersigned implicitly decided upon the necessity of it in the first place. Courts must be cautious when asked to issue search warrants prophylactically—that is, when the government maintains one is not required but still seeks one. Judges have the obligation to manage their dockets and conserve limited time and resources because "judicial economy plays a paramount role in trying to maintain an orderly, effective, administration of justice." *In re Vista print Ltd*., 628 F.3d 1342, 1346 (Fed. Cir. 2010). Here, the Court found that a search warrant was necessary and thus, authorized one. In the interest of addressing "largely-unexplored issues" that "will certainly arise again," *In re App. for Order Authorizing Disclosure of Location Info.*, 849 F. Supp. 526, 532 (D. Md. 2011), the undersigned "take[s] the opportunity to consider further the request and appropriate vehicles for such authorizations," *In the Matter of Search of a Cellular Telephone*, 430 F. Supp. 3d 1264, 1265 (D. Utah 2019).

Amendment require[d] the Government to obtain a warrant from a neutral magistrate to conduct [this] search." *United States v. Lambis*, 197 F. Supp. 3d 606, 611 (S.D.N.Y. 2016).

a. Fourth Amendment Search Doctrine and Cell Phone Location

The Supreme Court has recognized two tests to define searches. First, "Fourth Amendment search doctrine was [historically] 'tied to common-law trespass' and focused on whether the Government 'obtains information by physically intruding on a constitutionally protected area.'" *Carpenter*, 138 S.Ct. at 2213 (quoting *United States v. Jones*, 565 U.S. 400, 405, 406, n.3 (2012)). Second, the Court has more recently recognized that "a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable." *Kyllo v. United States*, 533 U.S. 27, 33 (2001). At bottom, the Fourth Amendment provides protection where the government has the opportunity to learn intimate facts about a person or a constitutionally protected area where it would otherwise have had to obtain a warrant to trespass upon that space, especially where the general public could not readily have learned such private information. *See United States v. Karo*, 468 U.S. 705, 715-16 (1984).

b. Cell-Site Simulator Technology and Fourth Amendment Searches

Cell-site simulator technology does not fit neatly into traditional conceptions of Fourth Amendment search and seizure doctrine.[5] The lack of clear information on the underlying

[5] At first blush, Fourth Amendment doctrine for cell site location information ("CSLI") appears most related. "[A]n individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI." *Carpenter*, 138 S. Ct. at 2217. "[H]istorical cell-site records present even greater privacy concerns than the GPS monitoring of a vehicle" because a cell phone "tracks nearly exactly the movements of its owner" wherever that person goes. *Id.* Furthermore, CSLI information "gives police access to a category of information otherwise unknowable:" the specific time and location of a person's whereabouts. However, *Carpenter* does not directly apply here. The Court specifically stated that its holding was "a narrow one" limited to historical CSLI data, and the Court disclaimed any view on "real-time CSLI or 'tower dumps.'" 138 S. Ct. at 2220. Cell-site simulators do not collect historical CSLI data, but instead offer a different method of single-instance real time surveillance by determining the signal strength and direction of the targeted cell phone.

technology behind cell-site simulators has led to a range of competing characterizations of their relationship with targeted cell phones. In one view, cell-site simulators simply "take advantage" of a cell phone's inherent function to constantly search for the "best cell tower available," suggesting that the cell-site simulator is a passive data collection device receiving the information cell phones naturally emit. *United States v. Temple*, 2017 WL 7798109 at *6 (E.D. Mo. Oct. 6, 2017). DOJ's guidance espouses this characterization. *See* DOJ Guidance, *supra*, at 2. Another view suggests that cell-site simulators are more active, stating that they "emit[] an especially strong signal [that] *induces* nearby cell phones to connect and reveal their direction relative to the device." *Patrick*, 842 F.3d at 542 (emphasis added). The Application takes a middle approach, stating that the cell-site simulator "electronically interrogates a cell phone prompting an automatic reply electronically as if it were in communication with an actual cell phone tower." Aff. 4, ECF No. 1. Regardless, a warrant is needed.

i. Trespass

The connection between a cell-site simulator and a phone is not an actual trespass because it does not involve a physical intrusion into a "constitutionally protected area." *Jones*, 565 U.S. at 407 (quoting *United States v. Knotts*, 460 U.S. 276, 286 (Brennan, J., concurring)). That is, the cell-site simulator never touches the targeted person or their property, without which there is no *trespass*-based search.

ii. Reasonable Expectation of Privacy

Cell-site simulators implicate individuals' reasonable expectations of privacy in information about constitutionally protected areas that otherwise could not be obtained without a search warrant. "'At the very core' of the Fourth Amendment 'stands the right of a [person] to retreat into [their] own home and there be free from unreasonable governmental intrusion.'" *Kyllo*,

533 U.S. at 31 (quoting *United States v. Silverman*, 365 U.S. 505, 511 (1961)). The use of a "cell-site simulator [may] reveal[] 'details of the home that would previously have been unknowable without physical intrusion,' namely, that the target cell phone was located within [the home]." *Lambis*, 197 F. Supp. 3d at 610 (quoting *Kyllo*, 533 U.S. at 40). The Application requested a 30-day period during which the government could employ the cell-site simulator with no restriction on where it may be targeted. "[T]here is no way to know before receipt of location data whether the phone [will be] physically located in a constitutionally-protected place." *In re Application for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel.*, 849 F. Supp. 2d 526, 540 (D. Md. 2011). Indeed, the Application acknowledges that the government can use a cell-site simulator determine the location of a target cell phone "even if it is located inside a house, apartment, or other building." Aff. 21, ECF No. 1. Thus, the possibility that a cell-site simulator may target a location in which a person has a "reasonable expectation of privacy" means that it necessarily "constitutes a Fourth Amendment search." *In re Application for an Order*, 849 F. Supp. 2d at 540; *see also Kyllo*, 533 U.S. at 38–39 (refusing to adopt a rule requiring a warrant for thermal imaging use only if it provided "intimate" details of the home because "no police officer would be able to know *in advance* whether his through-the-wall surveillance picks up 'intimate' details—and thus would be unable to know in advance whether it is constitutional").

c. Type of Warrant Required under Rule 41

The government properly applied for a traditional Rule 41 search warrant, *see* Appl., ECF No. 1, instead of a tracking-device warrant, *see* Rule 41(a)(2)(E). Cell-site simulators are not a "tracking device" as defined under 18 U.S.C. § 3117(b). Section 3117 discusses orders issued for the "*installation* of a mobile tracking device." § 3117(a) (emphasis added). Rule 41(e)(2)(c)

provides specific instructions on when the "*installation* authorized by the warrant" is to occur. F. R. Crim. P. Rule 41(e)(2)(C)(i), (ii) (emphasis added).

The plain meaning of "installation" and "device" indicate "the physical placement of some hardware or equipment." *United States v. Ackies*, 918 F.3d 190, 199 (1st Cir. 2019); *see In re Location Data Concerning an AT&T Cellular Tel.*, 102 F. Supp. 3d at 892.[6] "[A] cell phone used to track a person's movements is [not] a 'tracking device' under" § 3117 because the government does not physically install or place the targeted cell phone on the person or property of a suspect. *Ackies*, 918 F.3d at 1998. Moreover, "[t]he Supreme Court's general analogy of historical 'cell phone location information' to 'GPS monitoring' is not a holding that a cell phone is a 'tracking device' under an unmentioned statute." *Ackies*, 918 F.3d at 198 (quoting *Carpenter*, 138 S. Ct. at 2215–16).

When the government uses a cell-site simulator, it does not install, maintain, or remove the targeted cell phone from the suspect's person or property. *See* DOJ Guidance, *supra*, at 1.[7] Just as cell phones targeted through PLI warrants are not "tracking devices," neither are cell phones targeted through cell-site simulators. *Ackies*, 918 F.3d at 199. Although a cell-site simulator may allow the government to detect a suspect's cell phone in a given area and perhaps allow government agents to subsequently "track" the suspect, they are not "installed" when deployed for

[6] The Advisory Committee Notes for the 2006 Amendments to the Rules provide that Rule 41 tracking-device warrant provisions "include[] the authority to permit . . . *installation* of the tracking device, and maintenance and removal of the device." Advisory Committee Notes on 2006 Amendments to Fed. R. Crim. P. 41 (emphasis added). That the Advisory Committee contemplated "maintenance and removal" of tracking devices is further evidence that cell phone data collection tools are not tracking devices. *Ackies*, 918 F.3d at 200 (quoting Advisory Committee Notes on 2006 Amendments to Fed. R. Crim. P. 41).

[7] The government's Application also recognizes that cell-site simulators are not tracking devices under § 3117. Aff. 4, ECF. No. 1.

use. Cell-site simulators need not physically touch anything related to the suspect's person or property to receive signals from a targeted cell phone and help police determine its location. *See* DOJ Guidance at 1–2.[8]

III. Delayed Notice

Rule 41(f)(1)(C) requires the officer executing a warrant to give "a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken or leave a copy of the warrant and receipt at the place where the officer took the property." The government's Motion requested that the Court authorize the government to delay such notice to the charged fugitive—pursuant to 18 U.S.C. § 3103a(b)—for a period of 365 days. *See, e.g.*, Appl., ECF No. 1; Mot. 2, ECF No. 2. Rule 41(f)(3) provides that "[u]pon the government's request, a magistrate judge . . . may delay any notice required by this rule if the delay is authorized by statute," 18 U.S.C. § 3103a(b), creating what is commonly referred to as a "sneak and peak" warrant.

a. Requirements for Requests for Delay

Each of the three prongs of § 3103a(b) must be met for the court to authorize the government to delay notice to the Subscriber. First, the court must find "reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result." § 3103a(b)(1). "Adverse result" is defined under 18 U.S.C. § 2705, *inter alia,* as "flight from prosecution," "destruction of or tampering with evidence," or "otherwise seriously jeopardizing an investigation." § 2705(2)(B), (C), (E).

[8] One court suggested that a cell-site simulator was "akin to a warrant for a tracking device." *Johnson*, 2020 WL 6049562, at *15, *17. However, this court did not analyze the text of Rule 41 and § 3117, which speak to actual installation, not metaphorical.

"[T]he Fourth Amendment requires the issuing court to specify in writing that it made the determinations required by § 3103a(b)." *United States v. Espinoza*, No. CR-05-2075-7-EFS, 2005 WL 3542519, at *2 (E.D. Wash. Dec. 23, 2005); *see also United States v. Andrews*, No. 07-10221-02-MLB, 2008 WL 11396782, at *5 (D. Kan. May 16, 2008) (adopting *Espinoza*). "[A] bright-line rule requiring an issuing court to expressly make such findings is necessary, either by explicitly adopting and incorporating the affidavit's conclusions for the necessity for a § 3103a(b) warrant in a written order accompanying the warrant or on the warrant itself." *Espinoza*, 2005 WL 3542519, at *2. "The imposition of an explicit § 3103a(b) finding on the issuing court is supported by a comparison to the procedures utilized when an order is issued authorizing a wiretap under 18 U.S.C. § 2518." *Id.*

The Court denied the Motion and Amended Motion because the government failed to make an explicit reference to § 3103a(b) and plead an adverse result. The Government's Second Amended Motion cured this defect. *See* Second Am. Mot. 2–5, ECF No. 6. Thus, the Court granted the request for delayed notice.[9]

b. 365-Day Initial Delayed Notice Request in this Case Is Unreasonable

The USA PATRIOT Act mandates that sneak-and-peek warrants provide for notice "within a reasonable period not to exceed 30 days after the date of execution." § 3103a(b)(3). The court may extend this period to a later date "if the facts of the case justify a longer period of delay." *Id.* Such period of delayed notice "may be extended by the court for good cause shown, subject to the condition that extensions should only be granted upon an updated showing of the need for further

[9] The *Espinoza* court held that the remedy for failure to comply with § 3103a(b) was suppression. *See* 2005 WL 3542519, at *5. Strict compliance with § 3103a(b) is necessary to ensure "compliance with the Fourth Amendment." *Id.* Although the government cured the § 3103a(b) defects here, similar mistakes in the future may lead to the suppression of defective warrants.

delay and that each additional delay should be limited to periods of 90 days or less, unless the facts of the case justify a longer period of delay." § 3103a(c).

While these delayed notice provisions set no explicit boundaries on the initial or renewal "longer period of delay[s]," the default durations (30 days for initial requests and 90 days for extensions) reflect a view by Congress that shorter periods of delay are preferred. Such preference exists because there are "dangerous consequences to those whose [property is] searched and . . . seized surreptitiously without contemporaneous notice of the execution of a § 3103a warrant." *Espinoza*, 2005 WL 3542519, at *2. "[T]he Fourth Amendment[] demands that surreptitious entries be closely circumscribed." *United States v. Frietas*, 800 F.2d 1451, 1456 (9th Cir. 1986).

The government's initial Motion for delayed notice requested a period of nondisclosure of one year. *See* Mot. 2, ECF No. 2. The search here for a fugitive by deploying a cell site simulator for 30 days does not warrant the requested one-year initial delay. This is not a long-term investigation. Far from it, the limited purpose of the warrant is to find and apprehend the fugitive as soon as possible. If he is found within the 30 days the simulator is being used, he will be arrested right then pursuant to the extant arrest warrant. At or about that time, it would make sense to give notice of the seizure.

That the statute contemplates a short initial delay followed by renewals further points to Congressional aversion to such a lengthy delay up front. Given the weighty privacy issues at stake, inconvenience or administrative burden are not reasons to further delay notice. "It can be said with confidence that Congress has never indicated that it considers the giving of notice as a mere formality." *Application for Search Warrant for E-Mail Account [Redacted Text]@Gmail.com*

Maintained by Google, Inc., No. 10-mj-291 (AK/JMF), 2013 WL 12291516, at *5 (D.D.C. May 23, 2013).

The government cured its request for one-year delay by submitting its Second Amended Motion requesting delayed notice for a period of 30 days. Second Am. Mot. 7–8, ECF No. 6. Therefore, the undersigned approved the government's request. *See id.*

IV. Conclusion

A warrant for search and seizure is required to use a cell-site simulator to locate an individual, given there is no way of knowing whether the targeted cell phone will be found in a constitutionally protected area. Additionally, any request for delayed notice must explicitly discuss the elements of § 3103a(b) and demonstrate that they are satisfied.

Zia M. Faruqui

Digitally signed by Zia M. Faruqui
Date: 2021.03.25 08:03:49 -04'00'

ZIA M. FARUQUI
UNITED STATES MAGISTRATE JUDGE