IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF KANSAS

UNITED STATES OF AMERICA,

Plaintiff,

v.

ALBERT DEWAYNE BANKS *et al.*,

Defendants.

Case No. 13-cr-40060-DDC

MEMORANDUM AND ORDER

The government has filed a motion (Doc. 417) requesting that the Court issue three orders under 18 U.S.C § 2703(d) ("2703(d) orders") requiring Sprint, Verizon, and T-Mobile to disclose certain cell site location information ("CSLI") for phones the government wiretapped during this investigation. Defendants Johnson, Madkins, Thompson and Ponds have filed motions opposing the government's request. Docs. 418, 422, 425, 428. Other defendants have joined their opposition. Docs. 430, 436, 438. The government has filed a Reply. Doc. 429. In a nutshell, defendants argue that: (1) the "reasonable grounds" standard in 18 U.S.C. § 2703(d) is invalid under the Fourth Amendment; (2) the requested information is not "material to an ongoing criminal investigation" because, they assert, the government has closed the investigation; and (3) the government's motion is untimely because the government did not disclose the CSLI until after the July 1, 2014 deadline for suppression motions. For the reasons set forth below, the Court grants the government's motion for 2703(d) orders.

Background

Investigators obtained wiretap orders in the final months of a thirteen-month investigation into a suspected narcotics-trafficking conspiracy. The investigation was a joint effort by the Kansas Bureau of Investigation, the Junction City Police Department, the Geary County Sherriff's office, and the Riley County Police Department. Beginning in March of 2013, investigators submitted applications for wiretap orders to Judge Platt, a District Court Judge for Kansas' Eighth Judicial District. Judge Platt issued eight wiretap orders under the authority conferred by the Kansas wiretap statute, K.S.A. § 22-2514 *et seq*.

On August 22, 2014, this Court provisionally granted defendants' motions to suppress wiretap evidence on the basis that Judge Platt lacked authority to order interception of communications outside Kansas' Eighth Judicial District. The Court read K.S.A. § 22-2516(3) to require that either the tapped phones or the monitoring room be located in the district where the issuing judge presides. Because the monitoring room was located outside the Eighth Judicial District, the Court ruled that it must suppress the content of each intercepted phone call unless the government comes forward with evidence establishing that the tapped phones were physically located within Kansas' Eighth Judicial District at the time investigators intercepted each conversation. For this purpose, the government now seeks 2703(d) orders requiring electronic service providers to disclose CSLI relating to the tapped phones.

Analysis

A. The Stored Communications Act

Under the Stored Communications Act, 18 U.S.C. § 2701 *et seq.*, the government may require a cellular service provider to disclose subscriber records either by obtaining a warrant, *see* § 2703(c)(A), or by obtaining a court order. *See* § 2703(c)(B); § 2703(d). A court order

compelling a cellular service provider to disclose subscriber records does not require probable cause; rather, a court may issue a 2703(d) order upon "specific and articulable facts showing 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." § 2703(d).

The government seeks "[a]ll data about which 'cell towers' (i.e., antenna towers covering specific geographic areas) and 'sectors' (i.e., faces of the towers) received a radio signal from each [target phone during the period of interception]." *See, e.g.*, Doc. 422-1. In other words, the government seeks historical CSLI for each target phone during the time investigators intercepted communications transmitted over them. CSLI includes "records of calls made by the providers' customer . . . and reveals which cell tower carried the call to or from the customer." *United States v. Davis*, 754 F.3d 1205, 1211 (11th Cir. 2014). "The cell tower in use will normally be the cell tower closest to the customer. The cell site location information will also reflect the direction of the user from the tower. It is therefore possible to extrapolate the location of the cell phone user at the time and date reflected in the call record." *Id.* This information is distinct from GPS data, which the government has not requested.

The Court acknowledges that CSLI is less than a perfect method to establish the location of a target phone. *See, e.g., In re Application of the United States for an Order Authorizing Disclosure of Historical Cell Site Info. for Tel. Number*, __ F. Supp. 2d __, 2014 WL 1395082 (D.D.C. Apr. 17, 2014) (noting disagreement about how precisely CSLI can locate an individual). The legal standard adopted in this case, however, does not require the government to prove a target phone's location with pin-point accuracy—the government must only establish

that the target phone was present anywhere within Kansas' Eighth Judicial District. CSLI is probative for this purpose.

B. Constitutionality of The "Reasonable Grounds" Standard

Defendants argue that 18 U.S.C. § 2703(d) violates the Fourth Amendment because the statute authorizes a court to compel disclosure of CSLI upon "specific and articulable facts showing that there are reasonable grounds to believe" that the requested information is "relevant and material to an ongoing criminal investigation." *See* Docs. 418, 422, 425, 428. Because individuals have a legitimate expectation of privacy in CSLI, defendants argue, the Fourth Amendment prohibits the government from acquiring such information without a warrant supported by a showing of probable cause. Defendants rely upon the Eleventh Circuit's decision in *United States v. Davis*, 754 F.3d 1205, 1210-17 (11th Cir. 2014), *vacated and reh'g granted en banc*, No. 12-12928, 2014 WL 4358411 (11th Cir. Sept. 4, 2014). In that case, the Eleventh Circuit read the Supreme Court's opinions in *United States v. Jones*, __ U.S. __, 132 S. Ct. 945 (2012) to adopt a general "privacy theory" of the Fourth Amendment, which applies to prolonged collection of electronic location information. *Davis*, 754 F.3d at 1212.

In *Jones*, the Supreme Court found that that the government had conducted a search within the meaning of the Fourth Amendment when its investigators installed a GPS device on a suspect's car and tracked his location monitoring for a twenty-eight day period. 132 S. Ct. at 949. The majority opinion did not find a general expectation of privacy in location data, but instead relied on the fact that government agents had committed a trespass against the suspect's effects when they placed a GPS device on his car (the "trespass theory"). *Id.* at 952. Justice Alito, joined by four other justices, wrote a concurrence that relied exclusively on a privacy theory. *Id.* at 958 (Alito, J., concurring) (analyzing the issue "by asking whether respondent's

reasonable expectations of privacy were violated by the long-term monitoring of the movements of the vehicle he drove"). Justice Sotomayor, who concurred separately, discussed the possibility of applying a more generalized "privacy theory" to electronic location data but ultimately relied on the trespass theory "because the government's physical intrusion on [the defendant's] jeep supplies a narrower basis for decision." *Id.* at 957 (Sotomayor, J., concurring).

In *Davis*, the Eleventh Circuit considered all three opinions, noting that "[e]ven the opinion of the Court authored by Justice Scalia expressly did not reject the applicability of the privacy test." *Davis*, 754 F.3d at 1215. Reading the three *Jones* opinions together, the Eleventh Circuit determined that "the privacy theory is not only alive and well, but available to govern electronic information of search and seizure in the absence of trespass." *Id.* Applying the privacy theory to the facts in *Davis*, the Eleventh Circuit concluded that the use of CSLI to establish a suspect's location constitutes a search under the Fourth Amendment because (1) subscribers have an expectation of privacy in CSLI, and (2) subscribers do not "voluntarily" share CSLI information with third-party service providers. *Id.* at 1215-17. Law enforcement must therefore establish probable cause and obtain a warrant to track a suspect's location using CSLI. *Id.* at 1217.

Although the Tenth Circuit has not decided whether § 2703(d)'s "reasonable grounds" standard is constitutional, the Court concludes that the Tenth Circuit would not adopt the reasoning in *Davis.* The Eleventh Circuit's recent order vacating the decision to rehear the case en banc shows that the soundness of *Davis*'s holding is subject to question within even that circuit. *See United States v. Davis*, No. 12-12928, 2014 WL 4358411 (11th Cir. Sept. 4, 2014). Instead, to determine the constitutionality of § 2703's "reasonable ground standard," the Court follows the Fifth Circuit's analysis in *In re United States for Historical Cell Site Data*, 724 F.3d

600, 602 (5th Cir. 2013) (hereinafter "*Cell Site Data"*). In that case, the Fifth Circuit held that the government's acquisition of CSLI is not a search under the Fourth Amendment, and thus the Fourth Amendment's probable cause requirement does not apply to it. *Id.* at 615.

Significantly, the Fifth Circuit decided *Cell Site Data* after the Supreme Court had decided *Jones*. The Fifth Circuit distinguished *Jones* because, with CSLI, law enforcement is not the party collecting the data. *Id.* at 610. "[W]hen determining whether an intrusion constitutes a search or seizure," courts should distinguish "whether it is the Government collecting the information or requiring a third party to collect and store it, or whether it is a third party, of its own accord and for its own purposes, recording the information." *Id.* at 610. The government does not mandate that cellular service providers store CSLI and service providers may store or discard such data at their own discretion. *Id.* at 612. "And once an individual exposes his information to a third party, it can be used for any purpose, as '[i]t is established that, when a person communicates information to a third party even on the understanding that the communication is confidential, he cannot object if the third party conveys that information or records thereof to law enforcement authorities.'" *Id.* (citing *SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743 (1984)).

"In the case of such historical cell site information, the Government merely comes in after the fact and asks a provider to turn over records the provider has already created." *Id.* at 612. In this sense, a 2703(d) order compelling disclosure of CSLI is more like a subpoena of business records than it is law enforcement electronically tracking a suspect's movement and location, as in *Jones*. *Id.* But even viewing CSLI as a business record, a cellular service provider must have a "right to possession" in such records before a court can require it to turn the records over to law enforcement. *Id.* at 611. A third-party record keeper's right to possession in

CSLI depends on "whether the third party created the record to memorialize its business transaction with the target, rather than simply recording its observation of a transaction between two independent parties." *Id.* The Court concludes that here, as the Fifth Circuit held, the cellular service provider was an actual party to business transactions with the defendants. "The cell service provider collects and stores historical cell site data for its own business purposes, perhaps to monitor or optimize service on its network or to accurately bill its customers for the segments of its network that they use." *Id.* at 611-12. "Under this framework, cell site information is clearly a business record." *Id.* at 611.

Analyzed as a business record, a "conveyance of location information to the service provider nevertheless must be voluntary in order for the cell phone owner to relinquish his privacy interest in the data." *Cell Site Data*, 724 F.3d at 612. The Court finds that such conveyances are in fact, voluntary. "A cell service subscriber, like a telephone user, understands that his cell phone must send a signal to a nearby cell tower in order to wirelessly connect his call." *Id.* at 613 (citing *United States v. Madison*, No. 11-60285-CR, 2012 WL 3095357, at *8 (S.D. Fla. July 30, 2012). "Even if this cell phone-to-tower signal transmission was not 'common knowledge,'" cell service providers adopt contractual privacy policies and terms of use that "expressly state that a provider uses a subscriber's location information to route his cell phone calls." *Id.* at 613 (citing *California v. Greenwood*, 486 U.S. 35, 40 (1988); *Madison*, 2012 WL 3095357, at *8). These policies inform users that providers not only use CSLI, but also collect and record it. *See Madison*, 2012 WL 3095357 at *8. Although the defendants may *prefer* their location information to remain private, the Court does not believe that defendants reasonably could expect privacy because they voluntarily conveyed the information to third parties who openly collected and recorded it. "The Fourth Amendment, safeguarded by the

courts, protects only reasonable *expectations* of privacy." *Cell Site Data*, 724 F.3d at 615 (emphasis in original). Because the defendants voluntarily conveyed CSLI to service providers as part of a business transaction, the statutory standard in 2703(d) governs and Fourth Amendment protections do not apply to their CSLI.

C. Materiality of CSLI to an Ongoing Investigation

Having determined that 18 U.S.C. § 2703(d) contains a constitutionally appropriate standard, the Court turns to whether the government has met the standard adopted by this statute. Here, the only contested issue is whether the information sought is "relevant and material to an ongoing criminal investigation." Defendants argue that the government fails to meet this requirement for two reasons: (1) the information is not relevant to an "ongoing investigation" because the case is now in the prosecution state, and (2) the information is relevant to an evidentiary issue only, and not to substantive criminal charges. The Court addresses each argument, in turn, below.

The government claims that a "criminal investigation" continues well into trial. In support, the government points out that many investigatory activities continue into the prosecution stage, such as searching for hidden assets, identifying cooperators, and monitoring jail cells. Doc. 429 at 18. The government also argues that *Brady* case law recognizes that criminal investigations continue through the trial stage because *Brady* imposes a continuing obligation on the government to disclose evidence even after the investigation has moved to trial. *See United States v. Headman*, 594 F.3d 1179, 1183 (10th Cir. 2010) ("Although *Brady* claims typically arise from nondisclosure of facts that occurred before trial, they can be based on nondisclosure of favorable evidence (such as impeachment evidence) that is unavailable to the government until trial is underway."). In addition, even if the investigation had concluded, the

government asserts it has "reopened" its investigation for the purposes of requesting a 2703(d) order. *See* Doc. 417 at 4.

Defendants do not cite any authority for their argument that the return of an indictment terminates an investigation. Although the Court could not locate any cases interpreting 2703(d)'s "ongoing criminal investigation" requirement, courts have, albeit in different contexts, recognized that an investigation may continue beyond indictment. *See, e.g.*, *United States v. Phibbs*, 999 F.2d 1053, 1077 (6th Cir. 1993) ("Once a targeted individual has been indicted, the government . . . may [ ] continue to employ the grand jury process as part of an ongoing investigation, possibly leading to further charges against the subject of the former indictment."); *Times Mirror Co. v. United States*, 873 F.2d 1210, 1221 (9th Cir. 1989) ("We do not decide whether the public has a right of access to warrant materials . . . [when] an investigation is still ongoing, but an indictment has been returned."). Thus, the Court has no place second-guessing the government's assertion that it has reopened the investigation to determine the location of the target phones at certain times.

Defendants also argue that the CSLI is "relevant and material" to an evidentiary issue only and not to the substantive criminal charges. Their argument relies on basic definitions of the two terms— that information is "relevant" if it makes a fact "of consequence" more or less likely, Fed. R. Evid. 401, and that information is "material" if it has "some logical connection with consequential facts." *Black's Law Dictionary* 1124 (10th ed. 2014). Therefore, defendants claim, the government's request fails the "relevant and material" requirement because the information is relevant to a suppression motion only, and not to a "criminal investigation."

The Court does not read § 2703(d) so narrowly. Although the statute does not explicitly define the term "investigation," the statute does define "investigative officer" to include

attorneys involved in the prosecution of relevant offenses. 18 U.S.C. § 2510(7) ("Investigative or law enforcement officer" means any officer of the United States or of a State or political subdivision thereof, who is empowered by law to conduct investigations of or to make arrests for offenses enumerated in this chapter, and any attorney authorized by law to prosecute or participate in the prosecution of such offenses."). This definition suggests the statute contemplates that a "criminal investigation" includes the prosecution of target crimes. A broad interpretation also comports with the understanding that the purpose of investigating a crime is to discover evidence that a prosecutor can use to prosecute that crime. In sum, CSLI is clearly material and relevant to the prosecution because it supports the admissibility of other important, material evidence. The government's acquisition of CSLI therefore qualifies as part of an ongoing criminal investigation, and the Court rejects defendants' argument to the contrary.

Moreover, even if the Tenth Circuit would decide that the Fourth Amendment protects CSLI, the evidence before the Court is sufficient to support the issuance of a search warrant. "The fundamental objective that alone validates all unconsented government searches is, of course, the seizure of persons who have committed or are about to commit crimes, or of *evidence related to crimes*." *Illinois v. Rodriguez*, 497 U.S. 177, 184 (1990) (emphasis added). The government has established probable cause that defendants' phone calls are evidence of crimes on two levels. First, nearly a year of investigation provided enough evidence to support issuing wiretap orders, which "are often referred to as 'super-warrants' because of the additional requirements beyond probable cause necessary for their issuance." *In re Application of United States for an Order: (1) Authorizing Use of a Pen Register & Trap and Trace Device, (2) Authorizing Release of Subscriber and Other Info., (3) Authorizing Disclosure of Location-Based Servs.*, 727 F. Supp. 2d 571, 573 (W.D. Tex. 2010). Second, investigators collected additional

evidence of crimes once they began intercepting defendants' communications. *See* Doc. 395-1. By establishing that the phone calls are evidence of crimes, the government has also established probable cause for the related CSLI because such information reveals the defendants' location at the time of each call. *See Rodriguez*, 497 U.S. at 184.

The Court recognizes that a mere finding of probable cause does not satisfy the Fourth Amendment, and that the government must show probable cause by "oath or affirmation." *See* U.S. Const. Amend. IV ("no Warrants shall issue, but upon probable cause, supported by Oath or affirmation"); *In re Application of United States for an Order Authorizing Release of Historical Cell-Site Information*, 736 F. Supp. 2d 578, 579 (E.D.N.Y. 2010) (facts supporting probable cause "could not simply be proffered but would instead have to be established by means of an affidavit or affirmation"). The government has met the "oath or affirmation" requirement in this case. The record before the Court contains several affidavits supporting the wiretap applications, in which Special Agent Virden attests to facts establishing probable cause that intercepting defendants' communications would produce evidence of crimes. *See* Docs. 379-4, 379-6, 379-8, 379-12, 379-14, 379-16. The record also contains a voluminous affidavit for search warrants, in which Detective Babcock attests to the content and incriminating nature of intercepted calls. *See* Doc. 395-1. Thus, in addition to meeting the statutory requirements for a 2703(d), the Court concludes that the government has met the requirements for a search warrant under the Fourth Amendment.

D. Timing of the Government's 2703(d) Request

On June 6, 2013, Magistrate Judge Sebelius issued a scheduling order for this case. Judge Sebelius ordered the government to give notice of any intent to use evidence that defendants may seek to suppress. Doc. 46 at 7. The order also required the Government to

disclose evidence material to the preparation of a defense "at least 14 days before the deadline the court sets for the defendants to file motions to suppress and other pretrial motions and notices." *Id.* at 8. Defendants argue that if the government intended to use CSLI, it should have obtained and disclosed the evidence long ago. Defendants contend that it would be unfair for the government to acquire this information so close to trial because they have not had time to prepare suppression motions. To prepare a motion to suppress the CSLI, defendants claim that they will need to learn about the relevant technology, investigate how the different service providers collect CSLI, identify and retain an expert in the field, research and draft a motion to suppress, and hold another pretrial hearing. *See* Doc. 422 at 11-12. Defendants move, in the altenrative, that the Court should suppress the CSLI as a sanction for the government failing to comply with the scheduling order.

While the timing of the government's request for a 2703(d) order is not ideal, the Court finds the government did not violate the scheduling order because it did not have possess CSLI when the relevant deadlines passed. When determining whether to impose sanctions for failing to comply with a scheduling order, the Tenth Circuit has instructed district courts to consider the following factors: "(1) the reasons the government delayed producing the requested materials, including whether or not the government acted in bad faith when it failed to comply with the discovery order; (2) the extent of prejudice to the defendant as a result of the government's delay; and (3) the feasibility of curing the prejudice with a continuance." *United States v. Wicker*, 848 F.2d 1059, 1061 (10th Cir. 1988) (citing *United States v. Euceda-Hernandez*, 768 F.2d 1307, 1312 (11th Cir. 1985)). The government had no intention to use CSLI until defendants sought to suppress the evidence collected by the wiretaps and the Court ruled that establishing the location of the tapped phones was necessary to resolve the defendants' motions

to suppress. Defendants may argue that the government should have anticipated this issue, but the Court finds no basis to conclude that its failure to do so resulted from bad faith or other sanctionable neglect. The Court denies the defendants' argument that the government's motion for 2703(d) orders is untimely.

The Court will ensure that defendants have their opportunity to object to the admissibility of CSLI. The Court will consider any suppression motions filed within a reasonable time after this Order, and will schedule a hearing if necessary. Under a worst-case scenario, the Court will grant a continuance if doing so is necessary to consider defendants' objections to the admissibility of CSLI fully. However, simply denying the government access to important evidence is not the appropriate remedy for any timing difficulties that may result from the Court's issuance of 2703(d) orders.

IT IS THEREFORE ORDERED BY THE COURT THAT the government's motion for orders pursuant to 18 U.S.C. § 2703(d) (Doc. 417) is granted. The government shall present the Court with proposed 2703(d) orders within three days of the date of issuance of this Order.

IT IS SO ORDERED.

Dated this 15th day of September, 2014, at Topeka, Kansas.

s/ Daniel D. Crabtree
Daniel D. Crabtree
United States District Judge