

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF IDAHO**

IN THE MATTER OF APPLICATION FOR
SEARCH WARRANT OF REAL-TIME CELL
SITE LOCATION INFORMATION
MONITORING OF A CERTAIN
CELLPHONE

Case No. 1:19-ms-10530-S-REB

ORDER DENYING APPLICATION FOR
A SEARCH WARRANT

The undersigned has received two applications for search and seizure warrants from a law enforcement official authorized to apply for federal court search warrants pursuant to Rule 41 of the Federal Rules of Criminal Procedure (“Rule 41”). Each application seeks to utilize provisions of the Stored Communications Act (the “SCA”), 18 U.S.C. §§ 2701 *et seq.*, to obtain information from a wireless telephone service provider about a certain subscriber’s cellular phone, including the location of the phone over time. The subscriber, who will remain anonymous for purpose of this decision, is the subject of an outstanding federal arrest warrant issued out of the District of Idaho. The Government seeks the warrants to assist in locating the subject.

The first application seeks sixty days of historical subscriber data in various categories, including location data. This application is proper and if properly authenticated by the applicant, the Court is prepared to issue that requested warrant. It will not be further discussed in this decision.

The second application, however, seeks not historical location information or other historical subscriber data, but rather seeks thirty days of prospective “location information” regarding the target telephone. In other words, the Government seeks a warrant under the Stored Communications Act to permit the Government to gather future information, which the

application defines to include “all available E-911 Phase II data, GPS data, latitude-longitude data, and other precise location information, as well as 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 the cellular telephone.” Such location information is sometimes referred to as “real-time cell-site location information” or “real-time CSLI.” *Carpenter v. United States*, 138 S. Ct. 2206, 2220 (2018). This decision will refer to it generally as “prospective location information.”

The Court will deny the second application because the SCA does not authorize issuance of a warrant to allow the Government to collect prospective location information. The Court acknowledges that there are differing views about the application of the SCA to prospective location information and that different courts have ruled on both sides of the issue. The Ninth Circuit has not ruled on this issue, but a number of district courts, including within the Ninth Circuit, have considered the question. In *U.S. v. Espudo*, 954 F.Supp.2d 1029 (S.D. Cal. July 19, 2013), the court quoted extensively from *In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority*, 396 F.Supp.2d 747 (S.D. Tex. 2005) (“*2005 S.D. Tex. Application*”):

As implied by its full title (“Stored Wire and Electronic Communications and Transactional Records Access”), the entire focus of the SCA is to describe the circumstances under which the government can compel disclosures of existing communications and transaction records in the hands of third party service providers. Nothing in the SCA contemplates a new form of ongoing surveillance in which law enforcement uses co-opted service provider facilities.

Espudo, 954 F.Supp.2d at 1036 (quoting *2005 S.D. Tex. Application*, 396 F.Supp.2d at 760).

Still quoting the prior case, *Espudo* contrasted “wiretap and pen/trap orders, which are inherently prospective in nature” with SCA orders that are “inherently retrospective.” *Id.* Both cases then noted several distinctions between the SCA and the legal framework for wiretap and pen/trap

orders: the SCA does not specify a maximum surveillance period, it does not have a mechanism for extending SCA orders, and it does not impose ongoing reporting requirements. *Id.*

Furthermore, the cases held that the SCA “permits access to customer transaction records currently in the hands of the service provider, relating to the customer’s past and present use of the service.... [it] contemplates the production of existing records, not documents that may be created at some future date related to some future communication.” *Id.* at 1037. Ultimately, the court in the 2005 Southern District of Texas case concluded, and the *Espudo* court agreed, that “[i]f Congress had not intended the SCA to be retrospective in nature, it would have included the same prospective features it built into the wiretap and pen/trap statutes.” *Id.* In addition to adopting the reasoning from the earlier case, the *Espudo* court also noted that the use of the present tense in the statutory language of the SCA contemplates records that are already in existence. *Id.* The court also considered and rejected the so-called “hybrid theory” that there is statutory authority to obtain real-time cell site location data using a combination of the SCA and the Pen/Trap Statute, 18 U.S.C. § 3121 *et seq.* *Id.* After considering all of those aspects of the issue, the *Espudo* court held that “an application for real-time cell site location data does not implicate any statute regulating search or seizure or special circumstances. Accordingly, the terms of Rule 41 govern in the present case.” *Id.* at 1043. This Court agrees.

The same issue arose in *U.S. v. Cooper*, 2015 WL 881578 (N.D. Cal. Mar. 2, 2015). In that case, the court likewise rejected the Government’s argument that the SCA authorizes prospective location monitoring. After quoting from *Espudo*, the *Cooper* court held that Congress intended the SCA “to be used as a means to obtain data which has already been stored at the time the government seeks to obtain it. While the government relies primary on three cases ... which lend support to its ‘hybrid theory,’ the majority of courts have rejected it as an

attempt to circumvent the ... mandate that real time cell site data may be obtained only by a showing of probable cause.” *Id.* at *5 (collecting cases). The court held that the SCA does not authorize collecting prospective location information, noting that “[a] contrary decision would circumvent the very safeguards Congress meant to put in place by enacting the CALEA,” the statute that expressly precludes the Pen/Trap Statute from independently authorizing the real-time collection of location data.

In the matter now before this Court, the Government argues that the SCA, standing alone, authorizes the collection of prospective location information, relying upon *United States v. Ackies*, 918 F.3d 190 (1st Cir. 2019). The Court has considered the *Ackies* decision and finds that it is factually and legally distinct from the Government’s pending applications. In *Ackies*, the court held that two “precise location information warrants” to track the Defendant’s cell phones were properly issued under the SCA on a finding of probable cause. *Id.* at 194. The relevant challenges to the warrants on appeal in *Ackies* were whether a cell phone is a “tracking device” under 18 U.S.C. § 3117; whether geographic, jurisdictional limitations in Rule 41(b) barred the magistrate judge in the District of Maine from issuing the warrants for phones located outside Maine; and whether one of the two warrants was supported by probable cause. The court rejected each argument and upheld the legitimacy of the warrants.

None of these issues is directly implicated by the Government’s warrant application considered here. Rather, the precise issue presented here is whether the SCA authorizes the collection of prospective location information. Although *Ackies* affirmed the issuance of prospective location information warrants based on the SCA, the decision did not directly

confront this issue.¹ Thus, it is helpful to the Government only in its result, not in its analysis, because the decision does not address whether the SCA allows the Government to seek prospective location information.

The Court is not persuaded that the SCA authorizes collecting prospective location information. Rather, per *Espudo* and *Cooper*, the proper authority for a warrant application to collect prospective location information is Rule 41. As to that avenue, the Government contends that a warrant under Rule 41 “is not a viable alternative in this case” because there is no evidence that the subject’s cell phone is within the District of Idaho, and therefore the venue requirements of Rule 41(b) cannot be satisfied.² The Government notes that “if the Court declines to issue the warrant, the Government will have to rely on other less-direct and potentially less-effective methods to find” the subject.

The Court will accept the Government’s representation that the task of locating the suspect may be more cumbersome if the prospective location information warrant is not granted. But, of course, the Court is not privy to the information available to the Government about where the suspect may or may not be located.³ It is possible that the Government could properly seek a warrant in another District. Further, in certain circumstances the venue provisions of Rule 41(b) permit warrants which extend beyond the District Court in which they are issued, circumstances

¹ This Court infers that the *Ackies* court addressed only those arguments actually raised.

² Venue is broader under the SCA than under Rule 41. Under the SCA, “a court of competent jurisdiction,” 18 U.S.C. § 2703(c)(1)(A), including a court that “has jurisdiction over the offense being investigated,” 18 U.S.C. § 3127, may issue a warrant. Here, venue is proper under the SCA because the subject allegedly committed an offense within the District of Idaho – but the application must nonetheless be denied because the application is not properly brought under the SCA for the reasons discussed above. The venue restrictions of Rule 41(b) do not apply to warrants properly brought under the SCA.

³ However, the Government’s memorandum in support of its application states a belief that the subject is in either Florida or Washington.

which may be applicable to the Government's efforts here. Those details are, of course, unknown to the Court. But, under any scenario, the relative expediency or arguable cumbersomeness of the method of obtaining the location information sought by the Government is not a basis to rule that the SCA allows for something which its language otherwise does not permit.

Accordingly, the Government's application for a prospective location information warrant under the Stored Communications Act is **DENIED**.



DATED: September 6, 2019

A handwritten signature in black ink, appearing to read "Ronald E. Bush".

Honorable Ronald E. Bush
Chief U.S. Magistrate Judge